www.novell.com/documentation

Administration Guide

iFolder® 3.9.2

August 2015

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the Novell International Trade Services Web Page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2015 Novell, Inc. All rights reserved. Permission is granted to copy, distribute, and/or modify this document under the terms of the GNU Free Documentation License (GFDL), Version 1.2 or any later version, published by the Free Software Foundation with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the GFDL can be found at the GNU Free Documentation Licence (http://www.fsf.org/licenses/fdl.html).

THIS DOCUMENT AND MODIFIED VERSIONS OF THIS DOCUMENT ARE PROVIDED UNDER THE TERMS OF THE GNU FREE DOCUMENTATION LICENSE WITH THE FURTHER UNDERSTANDING THAT:

1. THE DOCUMENT IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE, OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY, ACCURACY, AND PERFORMANCE OF THE DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT IS WITH YOU. SHOULD ANY DOCUMENT OR MODIFIED VERSION PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL WRITER, AUTHOR OR ANY CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER; AND

2. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL THE AUTHOR, INITIAL WRITER, ANY CONTRIBUTOR, OR ANY DISTRIBUTOR OF THE DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER DAMAGES OR LOSSES ARISING OUT OF OR RELATING TO USE OF THE DOCUMENT AND MODIFIED VERSIONS OF THE DOCUMENT, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see The Novell Documentation Web page (http://www.novell.com/documentation/ifolder3).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list ((http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide **11**

1 Overview of Novell iFolder **13**

1.1 Benefits of iFolder for the Enterprise . . . 13
1.1.1 Seamless Data Access . . . 13
1.1.2 Data Safeguards and Data Recovery . . . 14
1.1.3 Reliable Data Security . . . 14
1.1.4 Encryption Support . . . 15
1.1.5 Productive Mobile Users . . . 15
1.1.6 Cross-Platform Client Support . . . 15
1.1.7 Scalable Deployment . . . 15
1.1.8 Multi-Server Support . . . 15
1.1.9 Multi-Volume Support . . . 16
1.1.10 Enhanced Web Administration . . . 16
1.1.11 No Training Requirements . . . 16
1.1.12 LDAP Group Support . . . 16
1.2 Benefits of iFolder for Users . . . 16
1.3 Enterprise Server Sharing . . . 18
1.4 Key Features of iFolder . . . 18
1.4.1 iFolder Enterprise Server . . . 18
1.4.2 iFolder Web Admin Console . . . 19
1.4.3 iFolder Web Access Console . . . 19
1.4.4 The iFolder Client . . . 19
1.4.5 Multi Server Support . . . 19
1.4.6 Encryption . . . 19
1.4.7 Shared iFolders . . . 20
1.4.8 iFolder Access Rights . . . 20
1.4.9 Account Setup for Enterprise Servers . . . 20
1.4.10 Access Authentication . . . 21
1.4.11 File Synchronization and Data Management . . . 21
1.4.12 Synchronization Log . . . 21
1.4.13 Upgrade Slave to Master . . . 21
1.4.14 iFolder Data Recovery Tool . . . 21
1.5 What's Next . . . 21

2 What's New in iFolder **23**

2.1 What's New in Novell iFolder 3.9.2 . . . 23
2.2 What's New in Novell iFolder 3.9.1 . . . 23
2.3 What's New in Novell iFolder 3.9 . . . 23
2.4 What's New in Novell iFolder 3.8.4 . . . 23
2.5 What's New in Novell iFolder 3.8 . . . 24
2.6 What's New in Novell iFolder 3.7 . . . 24
2.7 What's New in Novell iFolder 3.6 . . . 24

3 Planning iFolder Services **27**

3.1 Security Considerations . . . 27
3.2 Server Workload Considerations . . . 27
3.3 Naming Conventions for Usernames and Passwords . . . 28

3.3.1 LDAP Naming Requirement . . . 28
3.3.2 Multilingual Considerations . . . 29
3.4 Admin User Considerations . . . 29
3.4.1 iFolder Admin User and Equivalent Users . . . 29
3.4.2 iFolder Proxy User . . . 29
3.5 iFolder User Account Considerations . . . 30
3.5.1 Preventing the Propagation of Viruses . . . 30
3.5.2 Synchronizing User Accounts with LDAP . . . 31
3.5.3 Synchronizing LDAP Group Accounts with LDAP . . . 31
3.5.4 Setting Account Quotas . . . 32
3.6 iFolders Data and Synchronization Considerations . . . 33
3.6.1 Naming Conventions for an iFolder and Its Folders and Files . . . 33
3.6.2 Guidelines for File Types and Sizes to Be Synchronized . . . 33
3.7 Management Tools . . . 34
3.7.1 iFolder Configuration Plug-Ins for YaST . . . 34
3.7.2 Novell iFolder Web Admin for Novell iManager 2.7 . . . 35
3.7.3 Web Access Configuration File . . . 35
3.7.4 Installing iFolder Clients Through Novell ZENworks . . . 36

4 Comparing Novell iFolder 2.x with 3.9 37

4.1 Comparison of Server Features and Capabilities of 2.*x* with 3.9 . . . 37
4.2 Comparison of Client Features and Capabilities of 2.*x* with 3.9 . . . 40
4.3 Comparison of Web Access Features and Capabilities of 2.*x* with 3.9 . . . 43

5 Prerequisites and Guidelines 45

5.1 File System . . . 45
5.2 Enterprise Server . . . 45
5.2.1 Install Guidelines When Using a Linux POSIX Volume to Store iFolder Data . . . 45
5.2.2 Install Guidelines for Other Components . . . 45
5.3 NetIQ eDirectory 8.8.8 . . . 46
5.4 Active Directory . . . 46
5.5 Novell iManager 2.7 . . . 47
5.6 Mono . . . 47
5.7 Client Computers . . . 48
5.8 Web Browser . . . 48

6 Installing and Configuring iFolder Services 49

6.1 Installing iFolder on an Existing OES Server . . . 49
6.2 Deploying iFolder Server . . . 51
6.2.1 Configuring the iFolder Enterprise Server . . . 52
6.2.2 Configuring the iFolder Slave Server . . . 63
6.2.3 Managing Server IP Change . . . 70
6.3 Configuring the iFolder Web Access Server . . . 70
6.3.1 Configuring Web Access . . . 71
6.3.2 Configuring iFolder Web Access for iChain or AccessGateway . . . 72
6.4 Configuring the iFolder Web Admin Server . . . 72
6.4.1 Configuring Web Admin Console . . . 73
6.4.2 Configuring iFolder Web Admin for iChain or AccessGateway . . . 74
6.5 Configuring the iFolder Enterprise Server with Active Directory as an LDAP source . . . 74
6.6 Installing the Novell iFolder 3 Plug-In for iManager . . . 85
6.6.1 Prerequisites . . . 85
6.6.2 Installing a Plug-In When RBS Is Not Configured . . . 85
6.6.3 Installing a Plug-In When RBS Is Configured . . . 86
6.7 Recovery Agent Certificates . . . 87

6.7.1 Understanding Digital Certification . . . 87
6.7.2 Creating a YaST-based CA . . . 88
6.7.3 Creating Self-Signed Certificates Using YaST . . . 90
6.7.4 Exporting Self-Signed Certificates . . . 92
6.7.5 Exporting Self-Signed Private Key Certificates For Key Recovery . . . 93
6.7.6 Exporting eDirectory CA Certificate Using iManager . . . 94
6.7.7 Using KeyRecovery to Recover the Data . . . 94
6.7.8 Managing Certificate Change . . . 95
6.8 Accessing iManager and the Novell iFolder Web Admin . . . 95
6.9 Provisioning Users, Groups and iFolder Services . . . 96
6.9.1 Prerequisites . . . 97
6.10 Distributing the iFolder Client to Users . . . 98
6.10.1 Accessing the OES Welcome Page . . . 98
6.10.2 Downloading the iFolder Client . . . 98
6.10.3 Installing the iFolder Client . . . 99
6.11 Using a Response File to Automatically Create iFolder Accounts . . . 100
6.11.1 Response Files . . . 100
6.11.2 Using a Response File to Deploy the iFolder Client . . . 103
6.12 Updating Novell iFolder 3.9.x . . . 106
6.13 Updating Mono for the Server and Client . . . 106
6.14 Uninstalling iFolder Enterprise Server . . . 107
6.15 What's Next . . . 107

7 Migrating iFolder Services 109

8 Running Novell iFolder in a Virtualized Environment 111

8.1 What's Next . . . 111

9 Clustering iFolder Servers with Novell Cluster Services for Linux 113

9.1 Prerequisites for Clustering iFolder Services . . . 113
9.2 Installing Novell Cluster Services for Linux . . . 113
9.3 Configuring iFolder Servers on a NCS for Linux Cluster . . . 114
9.4 Updating Cluster Shared Pool Load and Unload Scripts . . . 116
9.5 Managing Cluster Resource for iFolder . . . 116
9.6 Sample Load Scripts for iFolder Clusters . . . 116
9.6.1 Linux POSIX File System . . . 116
9.6.2 NSS File System . . . 117
9.7 Sample Unload Scripts for iFolder Clusters . . . 118
9.7.1 Linux POSIX File System . . . 118
9.7.2 NSS File System . . . 118
9.7.3 Troubleshooting . . . 119
9.8 Sample Monitor Scripts for iFolder Clusters . . . 120
9.8.1 Linux POSIX File System . . . 120
9.8.2 NSS File System . . . 120

10 Managing an iFolder Enterprise Server 123

10.1 Starting iFolder Services . . . 123
10.2 Stopping iFolder Services . . . 123
10.3 Restarting iFolder Services . . . 123
10.4 Managing the Simias Log and Simias Access Log . . . 124
10.5 Backing Up the iFolder Server . . . 125
10.6 Recovering from a Catastrophic Loss of the iFolder Server . . . 126
10.7 Using TSAIF to Back Up and Restore the iFolder Store . . . 127

10.7.1 Understanding TSAIF . . . 127
10.7.2 Syntax . . . 128
10.7.3 iFolder Path Options . . . 128
10.7.4 iFolder Path Examples . . . 129
10.7.5 SMSConfig Options . . . 130
10.7.6 TSAIF and SMSConfig Examples . . . 131
10.7.7 NBackup Options . . . 131
10.7.8 TSAIF and NBackup Examples . . . 132
10.7.9 Additional Information . . . 133
10.8 Recovering iFolder Data from File System Backup . . . 133
10.8.1 Recovering a Regular iFolder . . . 133
10.9 Moving iFolder Data from One iFolder Server to Another . . . 134
10.10 iFolder Data Recovery Tool . . . 135
10.10.1 Understanding the iFolder Data Recovery Tool . . . 135
10.10.2 Prerequisites and Guidelines . . . 136
10.10.3 Using the Data Recovery Tool . . . 136
10.11 Changing The IP Address For iFolder Services . . . 142
10.12 Securing Enterprise Server Communications . . . 143
10.12.1 Using SSL for Secure Communications . . . 143
10.12.2 Configuring the SSL Cipher Suites and Protocol for the Apache Server . . . 143
10.12.3 Configuring the Enterprise Server for SSL Communications with the LDAP Server . . . 144
10.12.4 Configuring the Enterprise Server for SSL Communications with the iFolder Client . . . 144
10.12.5 Configuring the Enterprise Server for SSL Communications with the Web Access Server and Web Admin Server . . . 145
10.12.6 Configuring an SSL Certificate for the Enterprise Server . . . 145

11 Managing iFolder Services via Web Admin 147

11.1 Accessing the Novell iFolder Web Admin . . . 147
11.2 Connecting to the iFolder Server . . . 147
11.3 Managing Web Admin Console . . . 149
11.4 Managing the iFolder System . . . 150
11.4.1 Viewing and Modifying iFolder System Information . . . 150
11.4.2 Viewing Reprovisioning Status . . . 151
11.4.3 Configuring iFolder Administrators . . . 152
11.4.4 Configuring System Policies . . . 156
11.5 Managing iFolder Servers . . . 159
11.5.1 Searching For Servers . . . 160
11.5.2 Upgrading a Slave Server to a Master Server . . . 165
11.6 Securing Web Admin Server Communications . . . 166
11.6.1 Using SSL for Secure Communications . . . 166
11.6.2 Configuring the SSL Cipher Suites for the Apache Server . . . 166
11.6.3 Configuring the Web Admin Server for SSL Communications with the Enterprise Server 167
11.6.4 Configuring the Web Admin Server for SSL Communications with Web Browsers . . . 167
11.6.5 Configuring an SSL Certificate for the Web Admin Server . . . 168

12 Managing iFolder Users 169

12.1 Provisioning / Reprovisioning Users and LDAP Groups for iFolder . . . 169
12.1.1 Manual Provisioning . . . 169
12.1.2 Manual Reprovisioning . . . 170
12.1.3 Round-Robin Provisioning . . . 170
12.2 Searching for a User Account . . . 170
12.3 Accessing And Viewing General User Account Information . . . 171
12.3.1 Enabling or Disabling an iFolder For an User Account . . . 172
12.3.2 Deleting An iFolder . . . 172
12.4 Configuring User Account Policies . . . 172
12.4.1 Viewing the Current User Account Policies . . . 172

12.4.2 Modifying User Account Policies 174
12.5 Enabling and Disabling iFolder User Accounts 176

13 Managing iFolders 177

13.1 Accessing the iFolders Details Page 177
13.2 Viewing The iFolder Details 177
13.3 Searching for an iFolder 178
13.4 Managing iFolder Members 179
13.5 Managing an iFolder 179
13.5.1 Adding a Member 179
13.5.2 Understanding iFolder Access Rights 179
13.5.3 Setting the iFolder Access Right for a Member 180
13.5.4 Removing a Member 180
13.5.5 Transferring Ownership of an iFolder 181
13.5.6 Managing Orphaned iFolders 181
13.6 Managing iFolder Policies 181
13.7 Enabling and Disabling an iFolder 183

14 Managing an iFolder Web Access Server 185

14.1 Starting iFolder Web Access Services 185
14.2 Stopping iFolder Web Access Services 185
14.3 Distributing the Web Access Server URL to Users 185
14.4 Configuring the HTTP Runtime Parameters 185
14.5 Securing Web Access Server Communications 187
14.5.1 Using SSL for Secure Communications 187
14.5.2 Configuring the SSL Cipher Suites and Protocol for the Apache Server 187
14.5.3 Configuring the Web Access Server for SSL Communications with the Enterprise Server 188
14.5.4 Configuring the Web Access Server for SSL Communications with Web Browsers 189
14.5.5 Configuring an SSL Certificate for the Web Access Server 189

15 Troubleshooting Tips For Novell iFolder 191

15.1 On Upgrading the Server from OES 2 SP3 to OES 11, iFolder Fails to Function 192
15.2 iFolder Client on MAC Fails to Reconnect to the iFolder Server after Sleep 193
15.3 iFolder Slave Server Fails to Configure and Reports a 401 Unauthorized Error 193
15.4 iFolder Post Install on an Upgraded Server Might Result in Failure to Access iFolder Server 193
15.5 iFolder Server Configuration Fails on Upgrading to OES 11 SP1 server 193
15.6 Uploading of Files is Possible Only if the Secondary Administrator Sets the Disk Quota 193
15.7 Reprovisioning Users From One Server to Another Results in Creation of Duplicate Entries of iFolders for the Reprovisioned User 194
15.8 iFolder Does Not Support Spaces or Dots in the Admin DN and User Container DN 194
15.9 iFolder Deletion Leaves an Empty Directory on the Server 194
15.10 No Auto Upgrade For the iFolder Mac Client 194
15.11 Menus for the iFolder Client on Mac are Inconsistent with Menus on Windows and Linux 194
15.12 Unable to Create a New Account After Deletion of a Previous Account 195
15.13 The iFolder Icon Is Not Updated Automatically on SLES and SLED 11 195
15.14 Delta Sync Is Not Supported for Encrypted iFolders 195
15.15 The namcd Services Must Be Running While Changing the Proxy User Password by Using Common Proxy Script 195
15.16 The iFolder Web Admin Alias Name Does Not Support Spaces 195
15.17 iFolder Configuration Fails at Random 195
15.18 Setting Up the NSS file System Trustee Rights 196
15.19 Login to Web Admin and Web Access Console Fails with an Error Message 196

15.20 iFolder Full Restore Using nbackup fails to restore in a Cluster Environment 196
15.21 Exception Error When Datapath on Server is not Mounted 196
15.22 Temporary files are getting synchronized as actual files 197
15.23 Web Admin Console Fails to Start Up 197
15.24 Login to the Web Console Fails 197
15.24.1 Login Fails Randomly 197
15.24.2 A DSfW Server is Used as the LDAP Server. 197
15.25 The OES Common Proxy User Password is Not Always Compliant with the Password Policies . . 198
15.26 Enabling a Large Number of Users at the Same Time Times Out 198
15.27 Changes Are Not Reflected After Identity Sync Interval 198
15.28 Synchronizing a Large Number of Files Randomly Requires Multiple Sync Cycles 198
15.29 iFolder Data Does Not Sync and Cannot be Removed from the Server 198
15.30 Samba Connection to the Remote Windows Host Times out 199
15.31 Exception Error while Configuring iFolder on a Samba Volume. 199
15.32 LDAP Users Are Not Reflected in iFolder 199
15.33 Directory Access Exception on Creating or Synchronizing iFolders 199
15.34 Changing Permission to the Full Path Fails 199
15.35 List of Items Fails to Synchronize 199
15.36 Access Permission Error While Logging in Through Web Access 200
15.37 Web Admin and Web Access Show a Blank Page 200
15.38 Option to Start iFolder During System Login Does Not Work in the iFolder Client for SLED 11 . . . 200
15.39 On running simias-server-setup, the setup fails while configuring SSL 200
15.40 iFolder linux client fails to startup if the datapath does not have any contents 201
15.41 Incremental Patch Upgrade Issue in a Multiple-Server Scenario. 201

16 Frequently Asked Questions 203

16.1 iFolder 3.9 Server. 203
16.1.1 Is iFolder server for 3.9 supported on a 64-bit OS?. 203
16.1.2 Is iFolder going to support non-eDirectory related platforms as an identity source? 203
16.2 iFolder Client 203
16.2.1 Is iFolder 3.9.2 version supported on the Macintosh platform? 204
16.2.2 Can I use the iFolder 3.*x* client to connect to iFolder 3.9 server? 204
16.2.3 Can I can use iFolder 3.9 version on different operating systems on different workstations to access and share the files? 204
16.2.4 There was a 10 MB file limitation using Web Access? Is it still applicable for iFolder 3.9 version? 204
16.2.5 I deleted a file accidentally. Can I recover it?. 204
16.3 iFolder Administration 204
16.3.1 What is the management console for iFolder 3.9? 204
16.3.2 What are the new features in the Web Admin console? 205
16.3.3 Can the administrator control the ability to encrypt iFolder files? 205
16.3.4 Are there any enhancements for how bulk users are enabled for iFolder? 205
16.3.5 How can the iFolder administrator manage the data owned by an iFolder user who has been removed from the iFolder domain? 205

A Caveats for Implementing iFolder Services 207

A.1 iFolder User Move 207
A.2 Loading Certificates to the Recovery Agent Path 207
A.3 Using a Single Proxy User for a Multi-Server Setup 207
A.4 Slave Server Upgrade 208
A.5 Slave Configuration 208
A.6 Novell iFolder Admin User 208

B Decommissioning a Slave Server **209**

C Configuration Files **211**

C.1 Simias.config File . . . 211
C.2 Web.config File for the Enterprise Server . . . 212
C.3 Web.config File for the Web Admin Server . . . 214
C.4 Web.config File for the Web Access Server . . . 217

D Managing SSL Certificates for Apache **221**

D.1 Generating an SSL Certificate for the Server . . . 221
D.2 Generating a Self-Signed SSL Certificate for Testing Purposes . . . 222
D.3 Configuring Apache to Point to an SSL Certificate on an iFolder Server . . . 222
D.4 Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster . . . 223
D.5 Replacing the SSL Certificate for an iFolder Enterprise Server . . . 224
D.5.1 Replacing the SSL Certificate for a Single iFolder Server . . . 224
D.5.2 Replacing the SSL Certificate for an iFolder Master Server . . . 225
D.5.3 Replacing the SSL Certificate for an iFolder Slave Server . . . 225

E Product History of iFolder 3 **227**

E.1 Version History . . . 227
E.2 Network Operating Systems Support . . . 228
E.3 Workstation Operating Systems Support for the iFolder Client . . . 228
E.4 Server Client Support . . . 229
E.5 Web Server Support . . . 229
E.6 iFolder User Access Support . . . 230

F Documentation Updates **231**

F.1 August 2015 . . . 231
F.2 January 2014 . . . 231
F.2.1 Installing and Configuring iFolder Services . . . 231
F.2.2 Troubleshooting Tips For Novell iFolder . . . 232
F.2.3 Product History of iFolder 3 . . . 232
F.3 August 2012 . . . 232
F.3.1 What's New in iFolder . . . 232
F.3.2 Product History of iFolder 3 . . . 232
F.4 July 2011 . . . 232
F.4.1 Managing an iFolder Enterprise Server . . . 233
F.5 December 2010 . . . 233
F.5.1 Replacing the SSL Certificates . . . 233
F.6 June 2010 . . . 233
F.6.1 iFolder Data Recovery Tool . . . 233
F.6.2 Upgrade Slave to Master . . . 233
F.7 August 2009 . . . 234
F.7.1 Multi-Level Administration . . . 234
F.7.2 Active Directory Integration for iFolder . . . 234
F.7.3 Installation of iFolder on SLED and Windows Using ZENworks . . . 234
F.8 October 2008 . . . 235
F.8.1 LDAP Group Support . . . 235
F.8.2 Recovery Agent Certificates . . . 235
F.8.3 Recovering iFolder Data from File System Backup . . . 235
F.8.4 Viewing Reprovisioning Status . . . 236
F.8.5 SSL Communications . . . 236

F.8.6 Simias.config File 236
F.8.7 Web.config File for the Web Admin Server 237

About This Guide

This guide describes how to install, configure, and manage Novell iFolder enterprise server, Web Access server, Web Admin server, and the iFolder client. This guide is divided into the following sections:

- Chapter 1, “Overview of Novell iFolder,” on page 13
- Chapter 2, “What’s New in iFolder,” on page 23
- Chapter 3, “Planning iFolder Services,” on page 27
- Chapter 4, “Comparing Novell iFolder 2.x with 3.9,” on page 37
- Chapter 5, “Prerequisites and Guidelines,” on page 45
- Chapter 6, “Installing and Configuring iFolder Services,” on page 49
- Chapter 7, “Migrating iFolder Services,” on page 109
- Chapter 8, “Running Novell iFolder in a Virtualized Environment,” on page 111
- Chapter 9, “Clustering iFolder Servers with Novell Cluster Services for Linux,” on page 113
- Chapter 10, “Managing an iFolder Enterprise Server,” on page 123
- Chapter 11, “Managing iFolder Services via Web Admin,” on page 147
- Chapter 12, “Managing iFolder Users,” on page 169
- Chapter 13, “Managing iFolders,” on page 177
- Chapter 14, “Managing an iFolder Web Access Server,” on page 185
- Chapter 15, “Troubleshooting Tips For Novell iFolder,” on page 191
- Chapter 16, “Frequently Asked Questions,” on page 203
- Appendix A, “Caveats for Implementing iFolder Services,” on page 207
- Appendix B, “Decommissioning a Slave Server,” on page 209
- Appendix C, “Configuration Files,” on page 211
- Appendix D, “Managing SSL Certificates for Apache,” on page 221
- Appendix E, “Product History of iFolder 3,” on page 227
- Appendix F, “Documentation Updates,” on page 231

Audience

This guide is intended for system administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Novell iFolder 3.9.2 Administration Guide*, visit the Novell iFolder 3.*x* documentation Web site (http://www.novell.com/documentation/ifolder3).

Additional Documentation

For information, see the following:

- *Novell iFolder 3.x Security Administrator Guide* (http://www.novell.com/documentation/ifolder3/index.html)
- OES Content

  iFolder User Guide for Novell iFolder 3.9 (http://www.novell.com/documentation/ifolder3/index.html).
- Novell iFolder 3.*x* documentation (http://www.novell.com/documentation/ifolder3/index.html).

1 Overview of Novell iFolder

Novell iFolder 3.9 represents the next generation of iFolder, supporting multiple iFolders per user, user-controlled sharing, and a centralized network server for secured file storage and distribution. With iFolder, users' local files automatically follow them everywhere—online, offline, all the time—across computers. Users can share files in multiple iFolders, and share each iFolder with a different group of users. Users control who can participate in an iFolder and their access rights to the files in it. Users can also participate in iFolders that others share with them.

This section familiarizes you with the various benefits and features of iFolder and its main components:

- Section 1.1, "Benefits of iFolder for the Enterprise," on page 13
- Section 1.2, "Benefits of iFolder for Users," on page 16
- Section 1.3, "Enterprise Server Sharing," on page 18
- Section 1.4, "Key Features of iFolder," on page 18
- Section 1.5, "What's Next," on page 21

1.1 Benefits of iFolder for the Enterprise

Benefits of iFolder to the enterprise include the following:

- Section 1.1.1, "Seamless Data Access," on page 13
- Section 1.1.2, "Data Safeguards and Data Recovery," on page 14
- Section 1.1.3, "Reliable Data Security," on page 14
- Section 1.1.4, "Encryption Support," on page 15
- Section 1.1.5, "Productive Mobile Users," on page 15
- Section 1.1.6, "Cross-Platform Client Support," on page 15
- Section 1.1.7, "Scalable Deployment," on page 15
- Section 1.1.8, "Multi-Server Support," on page 15
- Section 1.1.9, "Multi-Volume Support," on page 16
- Section 1.1.10, "Enhanced Web Administration," on page 16
- Section 1.1.11, "No Training Requirements," on page 16
- Section 1.1.12, "LDAP Group Support," on page 16

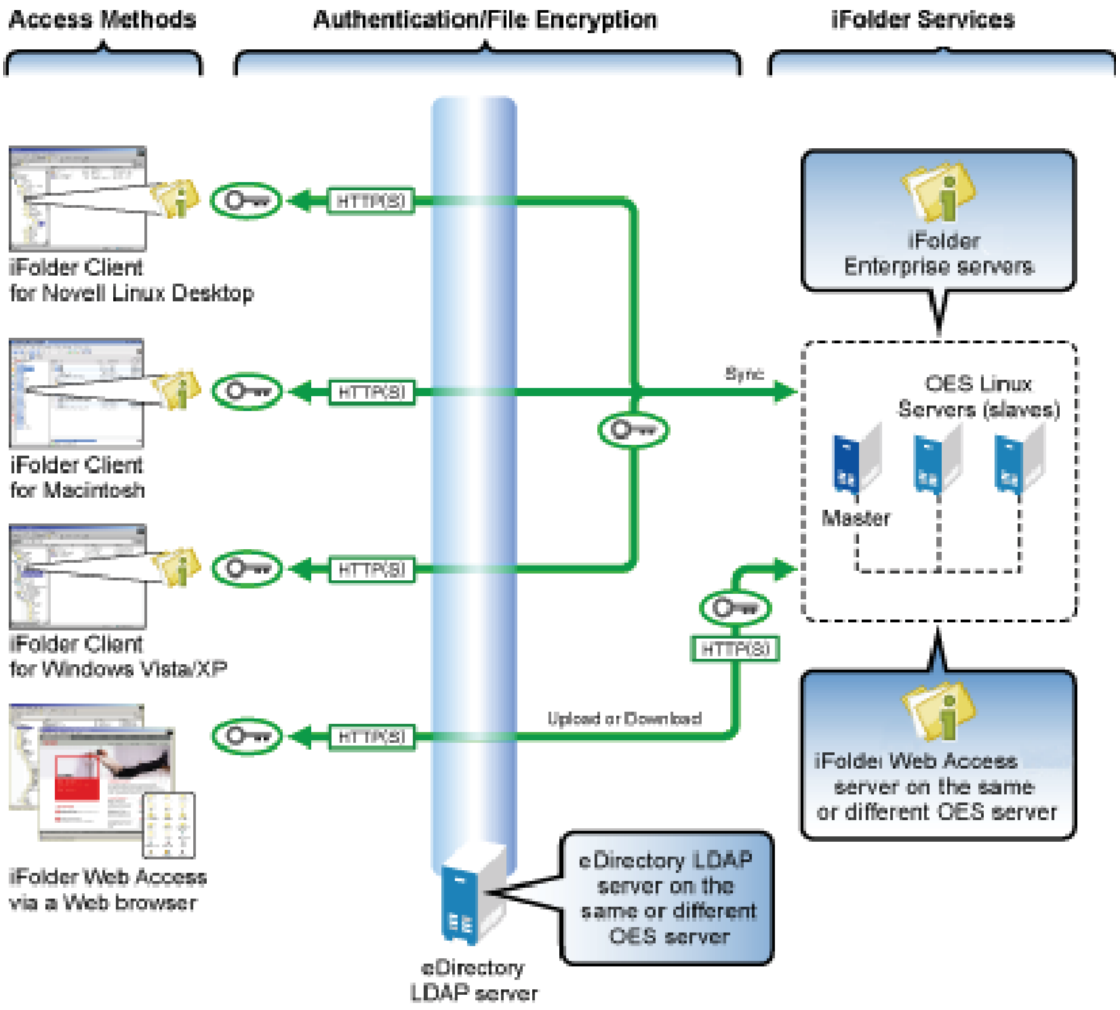
1.1.1 Seamless Data Access

Novell iFolder greatly simplifies the IT department's ability to keep users productive. It empowers users by enabling their data to follow them wherever they go.

The days of users e-mailing themselves project files so they can work on them from home are gone, along with the frustration associated with sorting through different versions of the same file on different machines. iFolder stores and synchronizes users' work in such a way that no matter what

client or what location they log in from, their files are available and in the condition that they expect them to be. Users can access the most up-to-date version of their documents from any computer by using the iFolder client or by using Web Access.

Figure 1-1 *Access Methods for Novell iFolder*



1.1.2 Data Safeguards and Data Recovery

With Novell iFolder, data stored on the server can be easily safeguarded from system crashes and disasters that can result in data loss. When a user saves a file to an iFolder on a local machine, the iFolder client can automatically update the data on the iFolder server, where it immediately becomes available for an organization's regular network backup operations. iFolder makes it easier for IT personnel to ensure that all of an organization's critical data is protected.

1.1.3 Reliable Data Security

With Novell iFolder, LDAP-based authentication for access to stored data helps prevent unauthorized network access.

1.1.4 Encryption Support

In a corporate environment, enterprise-level data is generally accessible to the IT department, which in turn can lead to intentional or unintentional access by unauthorized personnel. Because of this, executives have been hesitant to store some confidential documents on the network.

With encryption support, iFolder ensures higher security for users' confidential documents by encrypting them at the client side before transferring them to the server. Data is thus stored encrypted on the server, and is retrievable only by the user who created that iFolder.

iFolder makes it easier for IT managers to ensure that all of an organization's critical data is protected on the iFolder servers without involving any significant risks. iFolder also gives Internet Service Providers (ISPs) the ability to offer a user-trusted backup solution for their customers' critical business or personal data.

1.1.5 Productive Mobile Users

A Novell iFolder solution makes it significantly easier to support mobile users. VPN connections are no longer needed to deliver secure data access to mobile users. Authentication and data transfer use Secure Sockets Layer (SSL) technology to protect data on the wire.

Users do not need to learn or perform any special procedures to access their files when working from home or on the road. iFolder does away with version inconsistency, making it simple for users to access the most up-to-date version of their documents from any connected desktop, laptop, Web browser, or handheld device.

In preparation to travel or work from home, users no longer need to copy essential data to their laptop from various desktop and network locations. The iFolder client can automatically update a user's local computer with the most current file versions. Even when a personal computer is not available, users can access all their files via Web Access on any computer connected to the Internet.

1.1.6 Cross-Platform Client Support

The iFolder client is available for Linux, Macintosh, and Windows desktops. Web Access server for Novell iFolder provides a Web interface that allows users to access their files on the enterprise server through a Web browser on any computer with an active network or Internet connection.

1.1.7 Scalable Deployment

iFolder easily scales from small to large environments. You can install iFolder on multiple servers, allowing your iFolder environment to grow with your business. A single iFolder enterprise server handles unlimited user accounts, depending on the amount of memory and storage available. Users in an LDAP context can be concurrently provisioned for iFolder services simply by assigning the context to an iFolder server.

1.1.8 Multi-Server Support

Handling large amount of data and provisioning multiple enterprise users in a corporate environment is a major task for any administrator. iFolder simplifies these tasks with multi-server configuration. Multi-server support is designed exclusively for meeting your enterprise requirements. It serves the purpose of provisioning many users and hosting large amount of data on your iFolder domain. You can scale up the domain across servers to meet enterprise-level user requirements by adding

multiple servers to a single domain. This will allow you to leverage under-utilized servers in an iFolder domain. With multi-server deployment, thus, Enterprise level provisioning can be effectively managed and Enterprise level data can be scaled up.

1.1.9 Multi-Volume Support

One of the key features of iFolder is its storage scalability. With multi-volume support, Internet service providers and enterprise data centers can manage large amounts of data above the file system restrictions per volume. This facilitates moving data between the volumes, based on file size and storage space availability.

1.1.10 Enhanced Web Administration

Management of all iFolder enterprise servers is centralized through the enhanced iFolder Web Admin Console. Administrators can perform server management and maintenance activities from any location, using a standard Web browser. iFolder also frees IT departments from routine maintenance tasks by providing secure, automatic synchronization of local files to the server.

1.1.11 No Training Requirements

IT personnel no longer need to condition or train users to perform special tasks to ensure the consistency of data stored locally and on the network. With Novell iFolder, users simply store their files in the local iFolder directory. Their files are automatically updated to the iFolder server and any other workstations that share the iFolder. iFolder works seamlessly behind the scenes to ensure that data is protected and synchronized.

1.1.12 LDAP Group Support

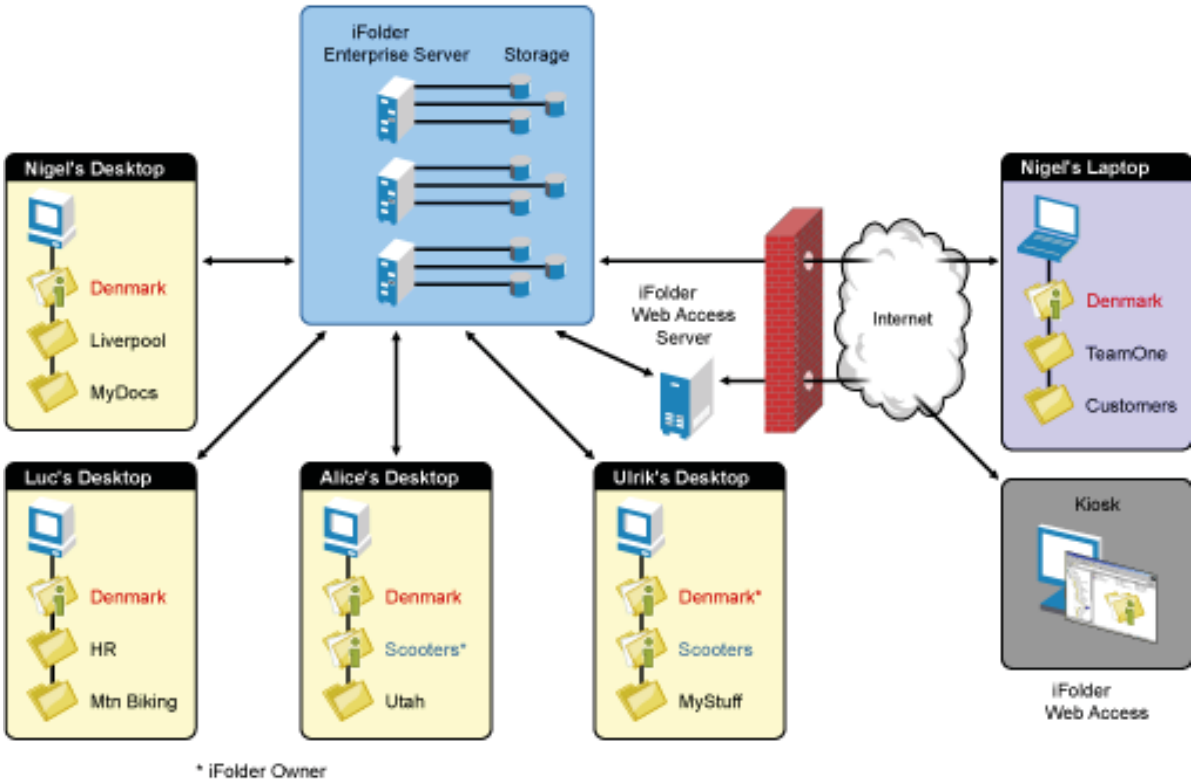
Provisioning and de-provisioning users separately becomes a difficult task when the total number of users is high. Even while sharing a particular file with 10 or 20 members of a same team, you need to select all members separately and then share. With the LDAP Groups feature, all the above problems are resolved. You can use the group facility for provisioning and de-provisioning, for setting same policy for a set of users. The users can share the iFolders with multiple users using groups.

1.2 Benefits of iFolder for Users

Typically, when users work in multiple locations or in collaboration with others, they must conscientiously manage file versions. With iFolder, the most recent version of a user’s files can follow the user to any computer where the iFolder client is installed and a shared iFolder is set up. iFolder also allows users to share multiple iFolders and their separate content with other users of the iFolder system. Users decide who participates in each shared iFolder, and also controls their level of access. Similarly, users can participate in shared iFolders that are owned by others in the collaboration environment.

In the following example, Ulrik owns an iFolder named Denmark and shares it via his iFolder enterprise account with Nigel, Luc, and Alice. Nigel travels frequently, so he also sets up the iFolder on his laptop. Any iFolder member can upload and download files from the Denmark iFolder from anywhere, using the iFolder Web Access server. In addition, Alice shares a non-work iFolder named Scooters with her friend Ulrik.

Figure 1-2 Collaboration and Sharing with iFolder



With an enterprise server, the iFolders are stored centrally for all iFolder members. The iFolder server synchronizes the most recent version of documents to all authorized users of the shared iFolder. All that the iFolder owner and iFolder members need is an active network connection and the iFolder client.

Novell iFolder provides the following benefits:

- Guards against local data loss by automatically backing up local files to the iFolder server and multiple workstations
- Prevent unauthorized network access to sensitive iFolder files.
- Allows multiple servers to participate in a single iFolder domain, to allow scaling up the number of users and data transfer bandwidth.
- Transparently updates a user's iFolder files to the iFolder enterprise server and multiple member workstations with the iFolder client
- Tracks and logs changes made to iFolder files while users work offline, and synchronizes those changes when they go online.
- Provides access to user files on the iFolder server from any workstation without the iFolder client, using a Web browser and an active Internet or network connection.
- With SSL encryption enabled, protects data as it travels across the wire.
- Makes files on the iFolder server available for regularly scheduled data backup.

1.3 Enterprise Server Sharing

The iFolder client included in this release supports synchronization across multiple computers through a central Novell iFolder enterprise server.

- Users can share files across computers.
- Users can share files with other users or groups.
- Each user can own multiple iFolders.
- User are allowed to set the encryption policy for their individual iFolder files.
- Each user can participate in multiple iFolders owned by other users.
- Files can be synchronized via the central server at any time and with improved availability, reliability, and performance.
- Data is transferred encrypted over the wire.
- Users are provisioned automatically for iFolder services based on their assignment to administrator-specified LDAP containers and groups. If there are multiple servers participating in a single domain, its users are balanced across the servers.
- A list of iFolder users is synchronized at regular intervals with the LDAP directory services.
- Local files are automatically backed up to the server at regular intervals and on demand.
- iFolder data on the server can be backed up to backup media and restored.
- Administrators can manage the iFolder system, user accounts, and user iFolders using the Novell iFolder 3 Web Admin.

1.4 Key Features of iFolder

- Section 1.4.1, “iFolder Enterprise Server,” on page 18
- Section 1.4.2, “iFolder Web Admin Console,” on page 19
- Section 1.4.3, “iFolder Web Access Console,” on page 19
- Section 1.4.4, “The iFolder Client,” on page 19
- Section 1.4.5, “Multi Server Support,” on page 19
- Section 1.4.6, “Encryption,” on page 19
- Section 1.4.7, “Shared iFolders,” on page 20
- Section 1.4.8, “iFolder Access Rights,” on page 20
- Section 1.4.9, “Account Setup for Enterprise Servers,” on page 20
- Section 1.4.10, “Access Authentication,” on page 21
- Section 1.4.11, “File Synchronization and Data Management,” on page 21
- Section 1.4.12, “Synchronization Log,” on page 21
- Section 1.4.13, “Upgrade Slave to Master,” on page 21
- Section 1.4.14, “iFolder Data Recovery Tool,” on page 21

1.4.1 iFolder Enterprise Server

The iFolder enterprise server is a central repository for storing iFolders and synchronizing files for enterprise users.

1.4.2 iFolder Web Admin Console

The iFolder Web Admin is an administrative tool used to manage the iFolder system, user accounts, and user iFolders and data.

1.4.3 iFolder Web Access Console

The iFolder Web Access console provides users with an interface for remote access to iFolders on iFolder enterprise server.

1.4.4 The iFolder Client

The iFolder client integrates with the user's operating system to provide iFolder services in a native desktop environment. It supports the following client operating systems:

- SUSE Linux Enterprise Desktop (SLED) 10 SP3
- SUSE Linux Enterprise Desktop (SLED) 11 SP3

  The iFolder Linux client requires the Mono framework for Linux and a GNOME desktop for iFolder Nautilus plug-in support.
- Windows XP SP3 32-bit
- Windows 7
- Windows 8
- Macintosh OS X 32-bit (Intel architecture) v10.6 and later (requires Mono 2.4.2.3). PowerPc architecture is not supported.

An iFolder session begins when the user logs in to an iFolder services account and ends when the user logs out of the account or exits the iFolder client. The iFolders synchronize files with the enterprise server only when a session is active and the computer has an active connection to the network or Internet. Users can access data in their local iFolders at any time; it does not matter if they are logged in to their server accounts or if they are connected to the network or Internet.

The iFolder client allows users to create and manage their iFolders. For information, see the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

1.4.5 Multi Server Support

Hosting large amounts of data as well as provisioning multiple users is necessary in any enterprise environment. In earlier versions of iFolder, the iFolder domain was dedicated to a single server, which limits the number of users and the hosting bandwidth. With multi-server support, iFolder 3.7 and later versions overcame these major limitations.

Multi-server support expands an iFolder domain across servers, so that the enterprise-level user provisioning can be effectively managed and enterprise-level data can be scaled up accordingly.

1.4.6 Encryption

Encryption support offers full security to iFolder users for their sensitive iFolder documents. Users can back up and encrypt their confidential files on the server without fear of losing it or having it exposed or falling into the wrong hands.

1.4.7 Shared iFolders

An iFolder is a local directory that the user selectively shares with other users in a collaboration environment. The iFolder files are accessible to all members of the iFolder and can be changed by those with the rights to do so. Users can share iFolders across multiple workstations and with others.

Because the iFolder client is integrated into the operating environment, users can work with iFolders directly in a file manager or in the My iFolders window. Within the iFolder, users can set up any subdirectory structure that suits their personal or corporate work habits. The subdirectory structure is constant across all member iFolders. Each workstation can specify a different parent directory for the shared iFolder.

1.4.8 iFolder Access Rights

The iFolder client provides four levels of access for members of an iFolder:

- **Owner:** Only one user serves as the owner. This is typically the user who created the iFolder. The owner or an iFolder Administrator can transfer ownership status from the owner to another user.

  The owner of an iFolder has the Full Control right. This user has Read/Write access to the iFolder, manages membership and access rights for member users, and can remove the Full Control right for any member. With an enterprise server, the disk space used by the owner's iFolders count against the owner's user disk quotas on the enterprise server.

  If a user is deleted from the iFolder system, the iFolders owned by the user are orphaned. Orphaned iFolders are assigned temporarily to the iFolder Admin user, who becomes the owner of the iFolder. Membership and synchronization continues while the iFolder Admin user determines whether an orphaned iFolder should be deleted or assigned to a new owner.
- **Full Control:** A member of the shared iFolder, with the Full Control access right. The user with the Full Control right has Read/Write access to the iFolder and manages membership and access rights for all users except the owner.
- **Read/Write:** A member of the shared iFolder, with the Read/Write access right to directories and files in the iFolder.
- **Read Only:** A member of the shared iFolder, with the Read Only access right to directories and files in the iFolder. This member can copy an iFolder file to another location and modify it outside the iFolder.

When used with an enterprise server account, the server hosts every iFolder created for that account. Users create an iFolder and the enterprise server makes it available to the specified list of users. A user can have a separate account on each enterprise server. A user's level of membership in each shared iFolder can differ.

1.4.9 Account Setup for Enterprise Servers

The iFolder client allows you to set up multiple accounts, with one each allowed per enterprise server. Users specify the server address, username, and password to uniquely identify an account. On his or her computer, a user sets up accounts while logged in as the local identity he or she plans to use to access that account and its iFolders. Under the local login, the user can set up multiple iFolder accounts, but each account must belong to a different iFolder enterprise server.

1.4.10 Access Authentication

Whenever iFolder connects to an enterprise server to synchronize files, it connects with HTTP BASIC and SSL connections to the server, and the server authenticates the user against the LDAP directory service.

1.4.11 File Synchronization and Data Management

When you set up an iFolder account, you can enable Remember Password so that iFolder can synchronize iFolder invitations and files in the background as you work. The iFolder client runs automatically each time you log in to your computer's desktop environment. The session runs in the background as you work with files in your local iFolders, tracking and logging any changes you make. With an enterprise server, you can synchronize the files at specified intervals or on demand.

1.4.12 Synchronization Log

The log displays a log of your iFolder background activity.

1.4.13 Upgrade Slave to Master

iFolder enables you to upgrade a slave server to a master server in a master-slave setup. You can achieve this by designating a slave server to be a master server from the Web Admin console.

1.4.14 iFolder Data Recovery Tool

The iFolder Data Recovery tool is a command line utility that enables you to restore backed-up files, folders, or iFolders for any user.

1.5 What's Next

Before you install iFolder, review the following sections:

- "Planning iFolder Services" on page 27
- "Prerequisites and Guidelines" on page 45

When you are done, install and configure your iFolder enterprise server and Web Access server.

2 What's New in iFolder

Novell iFolder 3.*x* and the iFolder client offer many new capabilities as compared to Novell iFolder 2.*x*. This section discusses the following:

- Section 2.1, "What's New in Novell iFolder 3.9.2," on page 23
- Section 2.2, "What's New in Novell iFolder 3.9.1," on page 23
- Section 2.3, "What's New in Novell iFolder 3.9," on page 23
- Section 2.4, "What's New in Novell iFolder 3.8.4," on page 23
- Section 2.5, "What's New in Novell iFolder 3.8," on page 24
- Section 2.6, "What's New in Novell iFolder 3.7," on page 24
- Section 2.7, "What's New in Novell iFolder 3.6," on page 24

2.1 What's New in Novell iFolder 3.9.2

The iFolder 3.9.2 service in OES 11 SP2 and OES 2015 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. There are no other changes in the OES 11 SP2 and OES 2015 release of iFolder.

2.2 What's New in Novell iFolder 3.9.1

The iFolder 3.9.1 service in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. There are no other changes in the OES 11 SP1 release of iFolder.

2.3 What's New in Novell iFolder 3.9

iFolder 3.9 service was modified to support Novell Open Enterprise Server 11. In addition, the following enhancements are added:

- Support for mono 2.6.7

2.4 What's New in Novell iFolder 3.8.4

The following features are new in iFolder 3.8.4:

- iFolder Data Recovery Tool. For more information, see Section 10.10, "iFolder Data Recovery Tool," on page 135.
- Upgrade a slave server to a master server. For more information, see Section 11.5.2, "Upgrading a Slave Server to a Master Server," on page 165.
- Support for OES common proxy. For more information on common proxy, refer to "Common Proxy User" in the *OES 11 SP2: Planning and Implementation Guide*.

2.5 What's New in Novell iFolder 3.8

The following features are new in iFolder 3.8:

- Multi-level administration. For more information, see "Multi-level administration" on page 152.
- Active Directory integration for iFolder. For more information, see Section 5.4, "Active Directory," on page 46.
- Support for mono 2.4 runtime environment.
- Passphrase recovery wizard. For more information, see section "Managing Passphrase for Encrypted iFolders" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*
- Support for changing iFolder account password using Web access console and iFolder clients.
- Enhanced User interface.
- Enhanced iFolder client startup performance.
- iFolder client for openSUSE 11.1 and SLED 11
- 64 bit version of iFolder client for Vista64.

2.6 What's New in Novell iFolder 3.7

The following features are new in iFolder 3.7:

- iFolder client for Macintosh and Vista
- Server Migration by using the Migration Tool
- SSL Communication
- LDAP Group Support
- Auto-Account creation by using a Response file
- iFolder Merge
- Improved file conflict management
- Enhanced Web administration
- Mechanism to re-provision users to another server

2.7 What's New in Novell iFolder 3.6

The following features are new in iFolder 3.6:

- Multi-sever support with no limit on the number of users and servers to allow expanding the iFolder domain across multiple servers
- Encryption support for users to store sensitive files secured on servers.
- Enhanced Web Admin console to manage, deploy and maintain iFolder system.
- Volume scalability support for iFolder servers to allow administrator to move data across multiple volume on a single server.
- With Multi-domain capability, iFolder 3.6 allows users to work with files belonging to two iFolders that reside on two different iFolder servers
- Enhanced web access for users to help them perform all the operations equivalent to that of iFolder client through web access. It allow mobile users access their iFolder and thus perform all the iFolder operations via mobile.

- Simplified iFolder sharing via Web Access.
- Enhanced reporting for better manageability.
- Support for multiple directories (eDirectory, OpenLDAP and SunOne)

3 Planning iFolder Services

This section discusses the planning considerations for providing Novell iFolder services.

- Section 3.1, “Security Considerations,” on page 27
- Section 3.2, “Server Workload Considerations,” on page 27
- Section 3.3, “Naming Conventions for Usernames and Passwords,” on page 28
- Section 3.4, “Admin User Considerations,” on page 29
- Section 3.5, “iFolder User Account Considerations,” on page 30
- Section 3.6, “iFolders Data and Synchronization Considerations,” on page 33
- Section 3.7, “Management Tools,” on page 34

3.1 Security Considerations

For information about planning security for your iFolder 3.*x* system, see the *Novell iFolder 3.9.2 Security Administration Guide*.

3.2 Server Workload Considerations

Novell iFolder supports a complex usage model where each user can own multiple iFolders and participate in iFolders owned by other users. Instead of a single user working from different workstations at different times, multiple users can be concurrently modifying files and synchronizing them. Whenever a user adds a new member to an iFolder, the workload on the server can increase almost as much as if you added another user to the system.

iFolder provides multi-server and multi-volume support to enhance the storage capability of its servers. Multi-Volume feature is exempt from the single iFolder per-volume restriction, so it enables you to move the data across multiple volume available on a single server. With the Web Admin console, you can add multiple mount points to a single server to increase the effective space available. The iFolder server also has the capability to configure the volume on which a particular iFolder needs to be created through the Web Admin console.

Multi-server support is a key feature that makes server workload management significantly easier for administrators. In the past, an iFolder domain was dedicated to a single server that limited the number of users and data transfer bandwidth. With multi-server support, iFolder has the capability to add more than one server to a single iFolder domain, so enterprise provisioning is effectively managed and hosting enterprise data is scaled up.

You can even set user account quotas to control the maximum storage space consumed by a user’s iFolders on the server. The actual bandwidth usage for each iFolder depends on the following:

- The number of members subscribed to the iFolder.
- The number of computers actively sharing the iFolder.
- How much data is stored in the iFolder.
- The actual and average size of files in the iFolder.
- The number of files in the iFolder.

- How frequently files change in the iFolder.
- How much data actually changes.
- How frequently files are synchronized.
- The available bandwidth and throughput of network connections.

We recommend that you set up a pilot program to assess your operational needs and performance based on your equipment and collaboration environment, then design your system accordingly.

The following is a suggested baseline configuration for iFolder server. It is based on an example workload of about 12.5 GB of data throughput (up and down) each 24 hours, including all Ethernet traffic and protocol overhead. Your actual performance might differ.

Table 3-1 *Suggested Baseline Configuration for an iFolder Enterprise Server*

Component	Example System Configuration
Hardware	1.8 GHz Single processor
	2 GB RAM
	300 GB hard drive
iFolder Services	500 users per server (multi-server configuration)
	500 MB user account quota per user
	1 iFolder per user that is not shared with other users
	5% change in each user's data per 24-hour period

If iFolder server is serving large number of requests, it is possible that for some requests you may receive HTTP 500 error. To manage this and to enable iFolder to serve more requests, do the following:

1. Edit the `/etc/security/limits.conf file` add the following lines:

   ```
   * soft nofile 100000
   * hard nofile 110000
   ```

2. Save the `limits.conf` file and reboot the server.

3.3 Naming Conventions for Usernames and Passwords

- Section 3.3.1, "LDAP Naming Requirement," on page 28
- Section 3.3.2, "Multilingual Considerations," on page 29

3.3.1 LDAP Naming Requirement

Usernames and passwords must comply with the constraints set by your LDAP service.

3.3.2 Multilingual Considerations

If you have workstations running in different languages, you might want to limit User object names to characters that are viewable on all the workstations. For example, a name entered in Japanese cannot contain characters that are not viewable in Western languages.

3.4 Admin User Considerations

During the iFolder install, iFolder creates two Administrator users, the iFolder Admin user and the iFolder Proxy user. After the install, you can also configure other users with the iFolder Admin right to make them equivalent to the iFolder Admin user.

- Section 3.4.1, “iFolder Admin User and Equivalent Users,” on page 29
- Section 3.4.2, “iFolder Proxy User,” on page 29

3.4.1 iFolder Admin User and Equivalent Users

The iFolder Admin user is the primary administrator of the iFolder enterprise server. Whenever iFolders are orphaned, ownership is transferred to the iFolder Admin user for reassignment to another user or for deletion. You initially specify the iFolder Admin user during the iFolder enterprise server configuration.

The iFolder Admin user must be provisioned to enable the iFolder Admin to perform management tasks. iFolder tracks this user by the LDAP object GUID, allowing it to belong to any LDAP container or group in the tree, even those that are not identified as LDAP Search contexts.

The iFolder Admin right can be assigned to other users so that they can also manage iFolder services for the selected server. Use the Web Admin console to add or remove the iFolder Admin right for users. Only users who are in one of the contexts specified in the LDAP Search contexts are eligible to be equivalent to the iFolder Admin user.

If you assign the iFolder Admin right to other users, those users are governed by the roster and LDAP Search DN relationship. The user is removed from the roster and stripped of the iFolder Admin right if you delete the user, remove the user’s DN from the list of LDAP Search contexts, or move the user to a context that is not in the LDAP Search contexts.

3.4.2 iFolder Proxy User

The iFolder Proxy user is the identity used to access the LDAP server to retrieve lists of users in the specified containers, groups, or users that are defined in the iFolder LDAP settings. This identity must have the Read right to the LDAP directory container configured during iFolder enterprise server setup. The iFolder Proxy user is created during the iFolder install and appropriate access rights are provided. You probably never need to modify this value. You can modify the Proxy user using the Web Admin console. For more information, see Step 7b on page 162 in the “Accessing and Viewing the Server Details Page” on page 160.

IMPORTANT: If you do modify the iFolder Proxy user, make sure that the identity you specify is different than the iFolder Admin user or other system users because the iFolder Proxy user password is stored in reversible encrypted form in the Simias database on the iFolder server. After you change the iFolder Proxy user, ensure that you restart Apache.

When you initially configure the iFolder enterprise server, iFolder autogenerates a password for the iFolder proxy user.

Table 3-2 Encryption Method for the iFolder Proxy User Password

iFolder Version	Encryption Method	iFolder Proxy User Password
iFolder 3.8.4	iFolder encryption method	Generates an alphanumeric, 21-digit mixed-case password.
iFolder 3.8	iFolder encryption method	Generates an alphanumeric, 21-digit mixed-case password.
iFolder 3.7	iFolder encryption method	Generates an alphanumeric, 21-digit mixed-case password.
iFolder 3.6	iFolder encryption method	Generates an alphanumeric, 21-digit mixed-case password.
iFolder 3.2	iFolder encryption method	Generates an alphanumeric, 13-digit, mixed-case password.
iFolder 3.0 and 3.1	BASH random number generator	Generates a number between `0` and `10,000` and appends it to iFolderProxy. For example, `iFolderProxy1234`.

Initially, the password for the iFolder Proxy user is stored in clear text in the `/datapath/simias/.local.ppf` file. At the end of the configuration process, the system reboots Apache 2 and starts iFolder. When iFolder runs this for the first time after configuration, the iFolder process encrypts the password and stores it in the Simias database and remove the entry from the `.local.ppf` file.

3.5 iFolder User Account Considerations

This section describes iFolder user account considerations.

- Section 3.5.1, “Preventing the Propagation of Viruses,” on page 30
- Section 3.5.2, “Synchronizing User Accounts with LDAP,” on page 31
- Section 3.5.3, “Synchronizing LDAP Group Accounts with LDAP,” on page 31
- Section 3.5.4, “Setting Account Quotas,” on page 32

3.5.1 Preventing the Propagation of Viruses

Because iFolder is a cross platform, distributed solution there is a possibility of virus infection on Windows machines when migrating data across the iFolder server to other platforms, and vice versa. You should enforce server-based virus scanning to prevent viruses from entering the corporate network.

You should also enforce client-based virus scanning. For information, see “Configuring Local Virus Scanner Settings for iFolder Traffic” in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

3.5.2 Synchronizing User Accounts with LDAP

You can specify any existing containers and groups in the *Search DNs* field of the iFolder LDAP settings. Based on the Search DNs, users are automatically provisioned with accounts for iFolder services.

The list of iFolder users is updated periodically when the LDAP synchronization occurs. New users are added to the list of iFolder users. Deleted users are removed from the list of iFolder users. (This might create orphaned iFolders if the deleted user owned any iFolders). If by mistake user is deleted from the LDAP, you can create that user again with the same FDN within the *Delete member grace interval* so that you can recover the user's iFolders. For more information on this, see Step 7 on page 161 in the "Accessing and Viewing the Server Details Page" on page 160.

IMPORTANT: Whenever you move a user between contexts and you want to provide continuous service for the user, make sure to add the target context to the list of LDAP Search DNs before you move the User object in eDirectory.

The LDAP synchronization tracks a user object's eDirectory GUID to identify the user in multiple contexts. It tracks as you add, move, or relocate user objects, or as you add and remove contexts as Search DNs.

The following guidelines apply:

- If the user is added to an LDAP container, group, or user that is in the Search DN, the user is added automatically to the iFolder user list.
- If a user is moved to a different container, and the new container is also in the Search DN, the user remains in the iFolder user list.

  If you intend to keep the user as an iFolder user without interruption of service and loss of memberships and data, the new container must be added as a Search DN before the user is moved.

  If the user is moved to a different container that is not specified as a Search DN before the user is moved, the user is removed from the iFolder user list. The user's iFolders are orphaned and the user is removed as a member of iFolders owned by others. If the new container is later added as a Search DN, the user is treated as a new user, with no association with previous iFolders and memberships.
- If the user appears in multiple defined Search DNs, and if one or more DNs are removed from the LDAP settings, the user remains in the iFolder user list if at least one DN containing the user remains.
- If the user is deleted from LDAP or moved from all defined Search DNs, the user is removed as an iFolder user. The user's iFolders are orphaned and the user is removed as a member of iFolders owned by others.
- The iFolder Admin user and iFolder Proxy user are tracked by their GUIDs, whether their user objects are in a context in the Search DN or not.

3.5.3 Synchronizing LDAP Group Accounts with LDAP

You can specify any existing containers and groups in the Search DNs field of the iFolder LDAP settings. Based on the Search DNs, LDAP Groups are automatically provisioned with accounts for iFolder services.

The list of LDAP Group is updated periodically when the LDAP synchronization occurs. New LDAP Groups are added to the list of iFolder users. Deleted LDAP Groups are removed from the list of iFolder users. (This might create orphaned iFolders if the deleted LDAP Group owned any iFolders).

If by mistake LDAP Group is deleted from the LDAP, you can create that LDAP Group again with the same FDN within the *Delete member grace interval* so that you can recover the user's iFolders. For more information on this, see Step 7 on page 161 in the "Accessing and Viewing the Server Details Page" on page 160.

IMPORTANT: Whenever you move a LDAP Group between contexts and you want to provide continuous service for the LDAP Group, make sure to add the target context to the list of LDAP Search DNs before you move the LDAP Group object in eDirectory.

The LDAP synchronization tracks a LDAP Group object's eDirectory GUID to identify the LDAP Group in multiple contexts. It tracks as you add, move, or relocate LDAP Group objects, or as you add and remove contexts as Search DNs.

The following guidelines apply:

- If the LDAP Group is added to an LDAP container, group, or LDAP Group that is in the Search DN, the LDAP Group is added automatically to the iFolder LDAP Group list.
- Any changes to the LDAP Group member list are automatically synchronized during next synchronization cycle.
- If an LDAP Group is moved to a different container, and the new container is also in the Search DN, the LDAP Group remains in the iFolder LDAP Group list.

  If you intend to keep the LDAP Group as an iFolder LDAP Group without interruption of service and loss of memberships and data, the new container must be added as a Search DN before the LDAP Group is moved.

  If the LDAP Group is moved to a different container that is not specified as a Search DN before the LDAP Group is moved, the LDAP Group is removed from the iFolder LDAP Group list. The LDAP Group's iFolders are orphaned and the LDAP Group is removed as a member of iFolders owned by others. If the new container is later added as a Search DN, the LDAP Group is treated as a new LDAP Group, with no association with previous iFolders and memberships.
- If the LDAP Group appears in multiple defined Search DNs, if one or more DNs are removed from the LDAP settings, the LDAP Group remains in the iFolder LDAP Group list if at least one DN containing the LDAP Group remains.
- If the LDAP Group is deleted from LDAP or moved from all defined Search DNs, the LDAP Group is removed as an iFolder LDAP Group. The LDAP Group's iFolders are orphaned and the LDAP Group is removed as a member of iFolders owned by others.
- The iFolder Admin LDAP Group and iFolder Proxy LDAP Group are tracked by their GUIDs, whether their LDAP Group objects are in a context in the Search DN or not.

NOTE: LDAP groups are not supported for OpenLDAP.

3.5.4 Setting Account Quotas

You can restrict the amount of space each user account is allowed to store on the server by setting an account quota. The account quota applies to the total space consumed by the iFolders the user owns. If the user participates in other iFolders, the space consumed on the server is billed to the owner of that iFolder. You can set quotas at the system or user level. Within a give account quota, you can also set a quota for any iFolder.

3.6 iFolders Data and Synchronization Considerations

Consider the following when setting policies for iFolders data and synchronization:

- "Naming Conventions for an iFolder and Its Folders and Files" on page 33
- "Guidelines for File Types and Sizes to Be Synchronized" on page 33

3.6.1 Naming Conventions for an iFolder and Its Folders and Files

The iFolder client imposes naming conventions that consider the collective restrictions of the Linux, Macintosh and Windows file systems. An iFolder, folder, or file must have a valid name that complies with the naming conventions before it can be synchronized.

Use the following naming conventions for your iFolders and the folders and files in them:

- iFolder supports the Unicode (http://www.unicode.org) character set with UTF-8 encoding.
- Do not use the following invalid characters in the names of iFolders or in the names of folders and files in them:

  `\/:*?"<>|;`

  iFolder creates a name conflict if you use the invalid characters in a file or folder name. The conflict must be resolved before the file or folder can be synchronized.
- The maximum name length for a single path component is 255 bytes. For filenames, the maximum length includes the dot (`.`) and file extension.
- Names of iFolders, folders, and files are case insensitive; however, case is preserved. If filenames differ only by case, iFolder creates a name conflict. The conflict must be resolved before the file or folder can be synchronized.
- If users create iFolders on the FAT32 file system on Linux, they should avoid naming files in all uppercase characters. The VFAT or FAT32 file handling on Linux automatically changes the filenames that are all uppercase characters and meet the MS-DOS 8.3 file format from all uppercase characters to all lowercase characters. This creates synchronization problems for those files if the iFolder is set with the Read Only access right.

3.6.2 Guidelines for File Types and Sizes to Be Synchronized

You can set policies to govern which files are synchronized by specifying file type restrictions and the maximum file size allowed to be synchronized. You can set these policies at the system, user account, and iFolder level.

Some file types are not good candidates for synchronization, such as operating system files, hidden files created by a file manager, or databases that are implemented as a collection of linked files. You might include only key file types used for your business, or exclude files that are likely unrelated to business, such as `.mp3` files.

Operating System Files

You should not convert system directories to iFolders. Most system files change infrequently and it is better to keep an image file of your basic system and key software than to attempt to synchronize those files to the server.

Hidden Files

If your file system uses hidden files to track display preferences, you should determine the file types of these files and exclude them from being synchronized on your system. Usually, they are relevant only to the particular computer where they were created, and they change every time the file or directory is accessed. You do not need to keep these files, and synchronizing them results in repeated file conflict errors.

For example, iFolder automatically excludes two hidden file manager files called `thumbs.db` and `.DS_Store`.

Database Files

iFolder synchronizes the changed portions of a file; it does not synchronize files as a set. If you have a database file that is implemented as a collection of linked files, do not try to synchronize them in an iFolder.

File Sizes

The maximum file size you allow for synchronization depends on your production environment. While some users work with hundreds of small files, other users work with very large files. You might set a system-wide policy to restrict sizes for most users, then set individual policies for power users.

3.7 Management Tools

Use the following tools to manage Novell iFolder enterprise servers and Web console servers.

- Section 3.7.1, “iFolder Configuration Plug-Ins for YaST,” on page 34
- Section 3.7.2, “Novell iFolder Web Admin for Novell iManager 2.7,” on page 35
- Section 3.7.3, “Web Access Configuration File,” on page 35
- Section 3.7.4, “Installing iFolder Clients Through Novell ZENworks,” on page 36

3.7.1 iFolder Configuration Plug-Ins for YaST

iFolder provides the following plug-ins to YaST for configuring basic parameters for your iFolder system:

iFolder Plug-In for YaST	Purpose	Tasks
iFolder 3	Use this function to configure the following parameters for the iFolder enterprise server. ◆ LDAP server name, LDAP admin DN, and password ◆ iFolder system name, store path, and description ◆ iFolder proxy DN, password, and search context for retrieving user information from LDAP ◆ iFolder admin DN and password	In YaST, *Open Enterprise Server > OES Install and Configuration> Novell iFolder* For information, see Section 6.2, “Deploying iFolder Server,” on page 51.

iFolder Plug-In for YaST	Purpose	Tasks
iFolder 3 Web Access	Use this function to configure the following parameters for the iFolder Web Access server. ◆ Web Access alias ◆ iFolder server URL	In YaST, *Open Enterprise Server > OES Install and Configuration> Novell iFolder > iFolder Web Access* For information, see Section 6.2, "Deploying iFolder Server," on page 51.
iFolder 3 Web Admin	Use this function to configure the following parameters for the iFolder Web Admin ◆ Web Admin alias ◆ iFolder server URL	In YaST, *Open Enterprise Server > OES Install and Configuration> Novell iFolder > iFolder Web Admin* For information, see Section 6.2, "Deploying iFolder Server," on page 51.

If both iFolder components are installed on the same computer, both plug-ins are available; otherwise, only the plug-in that is needed is available.

3.7.2 Novell iFolder Web Admin for Novell iManager 2.7

The Novell iFolder Web Admin is an administrative tool used to manage the iFolder system, user iFolder accounts, and user iFolders and data. For information about installing iManager, see the *Novell iManager 2.7 Installation Guide* (http://www.novell.com/documentation/imanager27/).

To access Novell iFolder 3, see Section 6.8, "Accessing iManager and the Novell iFolder Web Admin," on page 95.

Web Browser Language Setting

An iManager plug-in might not operate properly if the highest priority Language setting for your Web browser is set to a language other than one of the supported languages. To avoid problems, in your Web browser's Languages setting, set the first language preference in the list to a supported language, such as English.

Additional Information

For additional information, see the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/).

3.7.3 Web Access Configuration File

Use the `Web.config` file to configure HTTP runtime parameters for your iFolder Web Access server. For information, see Section 14.4, "Configuring the HTTP Runtime Parameters," on page 185.

3.7.4 Installing iFolder Clients Through Novell ZENworks

When an iFolder client is installed on a machine for the first time, iFolder Account Creation wizard is displayed automatically. New users may not always know details such as server name and user name to create a new account. In order to avoid this problem with client users, you can provide these details to the users automatically in some form. You can provide this information in many ways, one of which is ZENworks.

Using ZENworks, you can install the iFolder client and push the configuration file containing the details of user account to be created. For more information, see Section 6.11, “Using a Response File to Automatically Create iFolder Accounts,” on page 100.

4 Comparing Novell iFolder 2.x with 3.9

This section compares the features and capabilities of Novell iFolder 3.9 with Novell iFolder 2.*x*.

- Section 4.1, “Comparison of Server Features and Capabilities of 2.x with 3.9,” on page 37
- Section 4.2, “Comparison of Client Features and Capabilities of 2.x with 3.9,” on page 40
- Section 4.3, “Comparison of Web Access Features and Capabilities of 2.x with 3.9,” on page 43

4.1 Comparison of Server Features and Capabilities of 2.*x* with 3.9

Table 4-1 *Comparison of server features of 2.x with 3.9*

Feature or Capability	Novell iFolder 2.*x* Server	Novell iFolder 3.9 Enterprise Server
Server management	iFolder Administration tool `http://serveraddress/iFolderServer/Admin.html`	Web Admin console `http://serveraddress/admin`
Automatic provisioning of iFolder services	No The administrator enables iFolder services for users, requires users to log in to activate the account, and then creates the iFolder on the server.	Yes Multiple servers participate in a single iFolder domain and iFolder users are automatically balanced across participant servers.
Maximum iFolders per username	One	Multiple. Virtually unlimited number of iFolders as an owner or member.
Allows administrators to create an iFolder for a user	No	Yes
Allows administrators to share an iFolder and specify its member users	No	Yes ◆ For each iFolder, specify a list of users, which can be further modified by the iFolder owner. ◆ For each member of an iFolder, specify the user’s level of access with Full Control, Read/Write, and Read Only rights.
Allows administrators to transfer ownership of a shared iFolder to another user	No	Yes

Feature or Capability	Novell iFolder 2.*x* Server	Novell iFolder 3.9 Enterprise Server
LDAP Group Support	No	Yes LDAP group provisioning,de-provisioning, sharing,and setting Policies to group Objects is supported.
Detects orphaned iFolders and allows the iFolder Admin user to manage them	No	Yes
Maximum file size	Software limits file size to 4 GB. Below 4 GB, the maximum file size depends on the server's and clients' local file systems. For example, on Windows clients, FAT32 limits file sizes to 4 GB. On Linux, EXT2 limits file sizes to 2 GB.	There are no software restrictions, but the administrator can specify the maximum file size that users can synchronize as system-wide, individual user account quotas, and individual iFolder quotas. Below the administrative maximum, the practical maximum file size depends on the server's and clients' local file systems.
Maximum number of directories	32,765	No software restrictions; depends on the server's and clients' local file systems.
Disk quotas	The administrator can specify a default user quota that applies system-wide, and specify individual user quotas for iFolder accounts.	You can specify a default account quota that applies system-wide, individual user account quotas, and individual iFolder quotas. An owner can also specify a quota for an individual iFolder, but the total combined quotas for all the iFolders the user owns cannot exceed the system-wide account quota or the user's individual account quota, whichever is less. An iFolder member can specify a quota for the iFolder on each client. The quota cannot exceed the iFolder's quota or that user's own quota for his or her account.
Minimum synchronization interval	The administrator can set minimum synchronization intervals to apply system-wide and for individual users.	You can set minimum synchronization intervals to apply system-wide, for individual users, or for an individual iFolder.
Multi-volume support	No	With multi volume support, administrator can move the data across multiple volumes available on a single server. In effect, it ensure increased storage scalability.

Feature or Capability	Novell iFolder 2.*x* Server	Novell iFolder 3.9 Enterprise Server
Allows administrators to specify which file types to synchronize	No	Yes You can specify file types to include or exclude by setting system-wide, individual account, or individual iFolder policies.
Allows administrators to enable or disable the iFolder synchronization	Yes, by temporarily disabling iFolder services for the user account.	Yes, by using the iFolder Enable/ Disable User function to temporarily disable login for the user to the user's iFolder account.
Authenticated access	Yes, using the Admin username and password for the iFolder Management tool	Yes
Encrypted data transfer	Yes, with the encrypted iFolder option The Blowfish algorithm is applied with a user-specified passphrase. The admin user determines whether encryption services are available to users.	Yes, with automatic HTTPS (SSL) connections. The iFolder Admin user or equivalent determines whether secure or insecure connections are used.
iFolder data stored encrypted on server	Yes, with the encrypted iFolder option The user must specify a passphrase when first creating the iFolder account.	Yes
Backup of local files to a network server	Files in users' local iFolders are backed up on the iFolder server.	Files in users' local iFolders are backed up on the iFolder enterprise server.
Backup support to restore deleted files	Entire iFolder contents must be backed up and restored.	Individual files, directories, and iFolders are backed up.

4.2 Comparison of Client Features and Capabilities of 2.*x* with 3.9

Table 4-2 *Comparison of client features of 2.x with 3.9*

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.9 Enterprise Server
Download location	The iFolder download page is `http://serveraddress/iFolder` Replace *serveraddress* with the IP address or DNS name of your iFolder server. For example, `192.168.1.1` or `nifsvr1.example.com`. The path is case sensitive.	The administrator provides a download site where users can download the iFolder client.
Default location of the iFolder directory on a client	Windows: `C:\Documents and Settings\`*`username`*`\My Documents\iFolder\`*`username`*`\Home` Linux: `/home/userid/ifolder/userid` Macintosh: Not supported	`/home/username/`
Connect to server	Log in to one account at a time.	Set up accounts for multiple iFolder servers and log in to one or more as desired.
Authenticated access	Yes, with username and password authentication via your LDAP server.	Yes, with username and password authentication via your LDAP server.
Encrypted data transfer	Yes, with the encrypted iFolder option. The Blowfish algorithm is applied with a user-specified passphrase.	Yes, with automatic HTTPS (SSL) connections. You can control whether connections use HTTPS or HTTP.
iFolder data stored encrypted on server	Yes, with encrypted iFolder option The user must specify a passphrase when first creating the iFolder account.	Yes Data is stored encrypted on the server.
iFolder data stored encrypted on clients	No iFolder data is stored unencrypted on the client. Use third-party local encryption options, if needed.	No iFolder data is stored unencrypted on the client. Use third-party local encryption options, if needed.
Create an iFolder	Yes, by logging in to the server for the first time after being provisioned for iFolder services.	Yes, by selecting any local directory and making it an iFolder. A user can create multiple iFolders in each iFolder account.

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.9 Enterprise Server
Maximum iFolders per username	One	Multiple. Virtually unlimited number of iFolders as an owner or member.
Share an iFolder across multiple computers	Yes, by logging in to an iFolder server from a computer with the iFolder client, or by accessing the iFolder via the Web with NetStorage.	Yes, by logging in to an iFolder account from another computer with an iFolder client and setting up the available iFolder. You can select which of the iFolders you own or participate in to set up on each computer, according to your needs at each location.
Share an iFolder with other users	Not as designed, but it is possible. The administrator can create a username for this purpose. Membership in the iFolder is determined by who has access to the password for that username and its iFolder account.	Yes, as the owner user or a member user with the Full Control right. ◆ For each iFolder, specify a list of users. ◆ For each member of an iFolder, specify different levels of access with the Full Control, Read/Write, or Read Only right.
Share an iFolder with other LDAP groups	No	Yes You can share iFolders with other LDAP groups.
Participate in a shared iFolder owned by another user	Not as designed, but it is possible if the iFolder's owner shares his or her username and password. **IMPORTANT:** Sharing a password is a security risk and is never recommended.	Yes, if the owner adds you as a member. After the owner makes you a member of the iFolder, the server notifies you by making the iFolder available in your My iFolders window. Use the iFolder Setup function to activate the iFolder on one or more computers where you want to participate.
Allows the owner of a shared iFolder to transfer ownership of a shared iFolder to another user	No	Yes
Allows the iFolder owner to transfer ownership the iFolder to another user	No	Yes

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.9 Enterprise Server
Maximum file size	Software limits file size to 4 GB. Below 4 GB, the maximum file size depends on the server's and clients' local file systems. For example, on Windows clients, FAT32 limits file sizes to 4 GB. On Linux, EXT2 limits file sizes to 2 GB.	There are no software restrictions, but you can specify the maximum file size that users can synchronize as system-wide, individual user account quotas, and individual iFolder quotas. Below the administrative maximum, the practical maximum file size depends on the server's and clients' local file systems.
Restrict synchronization by including or excluding files by file type, such as `.mp3`	No	Yes, with policies set by you that can apply system-wide, to individual user accounts, or to individual iFolders.
Maximum number of directories	32,765	No software restrictions; depends on the server's and clients' local file systems.
Disk quotas	No	An owner can specify a quota for each iFolder, but the total combined administrative quotas for all owned iFolders cannot exceed the user's quota, or the system-wide quota if there is no user quota. An iFolder member can specify a quota for the iFolder on each computer where the iFolder is set up.
Minimum synchronization interval	The user sets a synchronization interval for each workstation. The value cannot be less than the system-wide setting or individual user setting.	The user sets a synchronization interval for each computer that applies to all iFolders in all accounts on that computer.
Allows users to suspend synchronization for a given client computer	Yes, using any of the following methods: ◆ Log out of the iFolder server ◆ Disable Automatic Synchronization in the Preferences tab. You can remain logged in, and then synchronization when you want with the Synchronization Now option.	Yes, using any of the following methods: ◆ Log out of the iFolder server account ◆ Disable Automatic Sync ◆ Disable the account in the Account window (deselect Enable Account)
Passphrase Management	No	Automated passphrase management.

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.9 Enterprise Server
Remote access to iFolder data on the server	Yes, using NetStorage. Your administrator must configure NetStorage for iFolder services.	Yes, using Web Access console.
Backup of local files to a network server	Files in users' local iFolders are backed up on the iFolder server.	Files in users' local iFolders are backed up on the iFolder enterprise server.
Backup support to restore deleted files	Administrators must back up and restore the entire iFolder contents.	You can back up the entire iFolder data store. You can restore individual files, directories, or iFolders.
Enhanced Web access	No	Management of all iFolder enterprise servers is centralized through the enhanced Web Admin. iFolder allows management from any location, using a standard Web browser.

4.3 Comparison of Web Access Features and Capabilities of 2.*x* with 3.9

Table 4-3 *Comparison Table*

Feature or Capability	Novell iFolder 2.*x* Web Access	Web Access Console for Novell iFolder 3.9
Web Access method	For iFolder 2.1.4 and earlier, the Java applet or Novell NetStorage For iFolder 2.1.5 and later, Novell NetStorage	Web Access console.

Web Access location	http://serveraddress/iFolder
	
	Replace *serveraddress* with the IP address or DNS name of your iFolder server. For example, `192.168.1.1` or `nifsvr1.example.com`. The path is case sensitive.
		`http://`*`serveraddress`*`/`
		`<`*`webalias`*`>`
		
		Replace *serveraddress* with the IP address or DNS name of your iFolder server. For example, `10.10.1.1` or `nifsvr1.example.com`.
		
		Replace *webalias* with the administrator-specified path. The default path is `/ifolder`. The path is case sensitive. For example:
		
		`http://10.10.1.1/ifolder`

Feature or Capability	Novell iFolder 2.*x* Web Access	Web Access Console for Novell iFolder 3.9
Connect to server	The user has only one iFolder per username. The user accesses the iFolder server where his or her files are located for that username.	Users separately access the different servers where you have accounts. All iFolders for the individual account are available.
Authenticated access	Yes, with username and password authentication via your LDAP server.	Yes, with username and password authentication via your LDAP server.
Encrypted data transfer	Yes, with the encrypted iFolder option.	Yes, with the encrypted iFolder option.
	The Blowfish algorithm is applied with a user-specified passphrase.	The Blowfish algorithm is applied with an auto-generated passphrase. An additional option is available to enable HTTPS(SSL) connection.
WebDAV protocol support	Yes, allows WebDAV clients, such as Microsoft Explorer, to seamlessly access folders and files on an iFolder 2.*x* server.	No

5 Prerequisites and Guidelines

This section discusses prerequisites and guidelines for using Novell iFolder server and the iFolder Client for version 3.9. Before installing and configuring iFolder, make sure that your system meets the requirements in each of the following:

- Section 5.1, “File System,” on page 45
- Section 5.2, “Enterprise Server,” on page 45
- Section 5.3, “NetIQ eDirectory 8.8.8,” on page 46
- Section 5.4, “Active Directory,” on page 46
- Section 5.5, “Novell iManager 2.7,” on page 47
- Section 5.6, “Mono,” on page 47
- Section 5.7, “Client Computers,” on page 48
- Section 5.8, “Web Browser,” on page 48

5.1 File System

We recommend that you store the users’ iFolder data on a separate volume.

5.2 Enterprise Server

- Section 5.2.1, “Install Guidelines When Using a Linux POSIX Volume to Store iFolder Data,” on page 45
- Section 5.2.2, “Install Guidelines for Other Components,” on page 45

5.2.1 Install Guidelines When Using a Linux POSIX Volume to Store iFolder Data

- In YaST, specify an Ext3 or ReiserFS partition as your system device.
- (Optional) Modify the Software components to add the iFolder 3 components to the install.

  If you install iFolder at this time, be prepared to configure iFolder as part of the install process. For more information, see Chapter 6, “Installing and Configuring iFolder Services,” on page 49.

5.2.2 Install Guidelines for Other Components

We recommend that your iFolder enterprise server, Web Admin server and Web Access server run on separate dedicated servers. For small office use, both enterprise server, Web Admin server and Web access server can run on the same server without degraded performance. For best performance, configure your iFolder server as an independent system with, at most, the following services:

- Directory services.

- Novell iFolder 3.9.x:
  - Enterprise server
  - Web Access server
  - Web Admin server
  - mono-addon version 2.6.7 (The Mono package is required for iFolder enterprise server, Web Admin server, and Web Access server.)
  - Apache 2 Web Server (The apache2-worker package is required for iFolder enterprise server, Web Admin server, and Web Access server.)

  IMPORTANT: Ensure that Apache is SSL-enabled and is configured to point to an SSL certificate on an ifolder server. For more information, see Section D.3, "Configuring Apache to Point to an SSL Certificate on an iFolder Server," on page 222.

Installing other applications or services on the iFolder server affects iFolder performance and might introduce conflicts with the required versions of applications iFolder depends on, such as Apache 2 or Mono.

5.3 NetIQ eDirectory 8.8.8

eDirectory 8.8.x is a secure identity management solution that provides centralized identity management, infrastructure, Net-wide security, and scalability to all types of applications running behind and beyond the firewall. It natively supports the directory standard Lightweight Directory Access Protocol (LDAP) 3 and provides support for TLS/SSL services based on the OpenSSL source code. eDirectory is available as a component of Novell Open Enterprise Server.

IMPORTANT: Ensure that you select *Use eDirectory Certificate for HTTPS services* option in the eDirectory configuration for a proper SSL communication between the iFolder master and the slave servers.

Before you configure iFolder, eDirectory must be configured and running. In iFolder, you specify LDAP containers and groups that contain User objects of users who you want to be iFolder users. You must create contexts and define users in eDirectory. For information, see the following topics in the *Novell eDirectory 8.8 Administration Guide* (https://www.novell.com/documentation/edir88/edirxdas_admin/data/bookinfo.html):

- "Designing Your Novell eDirectory Network" (http://www.novell.com/documentation/edir88/edir88/data/a2iiido.html)
- "Managing User Accounts" (http://www.novell.com/documentation/edir88/edir88/data/afxkmdi.html)

Make sure your LDAP objects comply with the naming conventions for your LDAP services. For information, see Section 3.3, "Naming Conventions for Usernames and Passwords," on page 28.

5.4 Active Directory

If you are using Active Directory as the LDAP source for iFolder, consider the following guidelines:

- During iFolder server configuration, you must select the *Require a secure connection between the LDAP server and the iFolder Server* option.

- Ensure that iFolder proxy user is assigned read rights on the configured user containers and attributes of user objects.
- For all users, the *User must change password at next login* option must not be set. Setting this option will lead to a login failure and an appropriate message will be displayed in the `Simias.log` file.
- When you specify the LDAP proxy DN in YaST, user with same name (for example, cn=iFolderProxy) must not exist in any other container
- Active Directory server must be SSL-enabled.

For information on how to configure Active Directory as an alternate LDAP server, see Section 6.5, "Configuring the iFolder Enterprise Server with Active Directory as an LDAP source," on page 74.

5.5 Novell iManager 2.7

Novell iManager 2.7 is a Web-based administration console that provides secure, customized access to network administration utilities and content. Before you can configure the Novell iFolder 3 Web Admin for iManager, iManager must be installed and configured.

For information, see the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/).

5.6 Mono

Novell iFolder requires the Mono framework for Linux. Mono is a development platform for running and developing modern applications. Based on the ECMA/ISO Standards, Mono can run existing programs that target the .NET or Java frameworks. The Mono Project is an open source effort led by Novell and is the foundation for many new applications. For information about Mono, see the Mono Project Web site (http://www.mono-project.com/Main_Page).

The required version of Mono is included in the `.iso` files. Mono is installed automatically as a dependency of iFolder during the install of the iFolder enterprise server or the Web Access server.

The iFolder client for Macintosh requires Mono 2.4.2.3. Linux and Macintosh users must install both iFolder and Mono packages. For information, see "Getting Started" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

Novell iFolder 3.9 supports mono-addon version 2.6.7 which is included in its install software. This package is explicitly bundled, installed, and used only by iFolder. Any updates to this package will only be available from OES patch channel. You cannot configure iFolder with any other version of mono installed on your system.

NOTE: When the iFolder server is running, you must not delete the `/tmp` folder because mod_mono stores some files in the `/tmp` folder. If you delete this folder, the iFolder server will become unusable. As a workaround, you must do the following:

1. Stop apache.

   ```
   /etc/init.d/apache2 stop
   ```

2. Stop the iFolder mono process.

   ```
   pkill mono
   ```

3. Start apache

   ```
   /etc/init.d/apache2 start
   ```

5.7 Client Computers

The iFolder client supports the following workstation operating systems:

- SUSE Linux Enterprise Desktop (SLED) 10 SP3
- SUSE Linux Enterprise Desktop (SLED) 11 SP3

  NOTE: The iFolder Linux client requires the Mono framework for Linux and a GNOME desktop for iFolder Nautilus plug-in support.

- Windows XP SP3 32-bit
- Windows 7
- Windows 8
- Macintosh OS X 32-bit (Intel architecture) v10.6 and later (requires Mono 2.4.2.3). PowerPc architecture is not supported.

Mono 2.4.2.3 is necessary to run the iFolder client for Macintosh. You can download and install Mono from OES Welcome page.

5.8 Web Browser

You need one or more of the following supported Web browsers on the computer you use to access Web Admin console, and Web Access console on the client computers:

- Mozilla Firefox 2.*x* and later
- Microsoft Internet Explorer
- Safari

6 Installing and Configuring iFolder Services

This section describes how to install and configure Novell iFolder Enterprise and Web console servers.

- Section 6.1, “Installing iFolder on an Existing OES Server,” on page 49
- Section 6.2, “Deploying iFolder Server,” on page 51
- Section 6.3, “Configuring the iFolder Web Access Server,” on page 70
- Section 6.4, “Configuring the iFolder Web Admin Server,” on page 72
- Section 6.5, “Configuring the iFolder Enterprise Server with Active Directory as an LDAP source,” on page 74
- Section 6.6, “Installing the Novell iFolder 3 Plug-In for iManager,” on page 85
- Section 6.7, “Recovery Agent Certificates,” on page 87
- Section 6.8, “Accessing iManager and the Novell iFolder Web Admin,” on page 95
- Section 6.9, “Provisioning Users, Groups and iFolder Services,” on page 96
- Section 6.10, “Distributing the iFolder Client to Users,” on page 98
- Section 6.11, “Using a Response File to Automatically Create iFolder Accounts,” on page 100
- Section 6.12, “Updating Novell iFolder 3.9.x,” on page 106
- Section 6.13, “Updating Mono for the Server and Client,” on page 106
- Section 6.14, “Uninstalling iFolder Enterprise Server,” on page 107
- Section 6.15, “What’s Next,” on page 107

6.1 Installing iFolder on an Existing OES Server

We recommend that you install iFolder after your server operating system is installed and all storage services are configured. The following procedure describes how to install iFolder enterprise server, iFolder Web access server, or both of the servers on an existing OES platform. If you install only one of the iFolder servers, repeat the entire install process for the other on a second OES server.

NOTE: If you used the Minimum install option for your OES server, which has no GUI installed, the iFolder services configuration is done with the YaST 2 text-based interface. For example, there are no check boxes and clicking is not possible. Use the standard methods for navigating the text-based interface to achieve the tasks as described here.

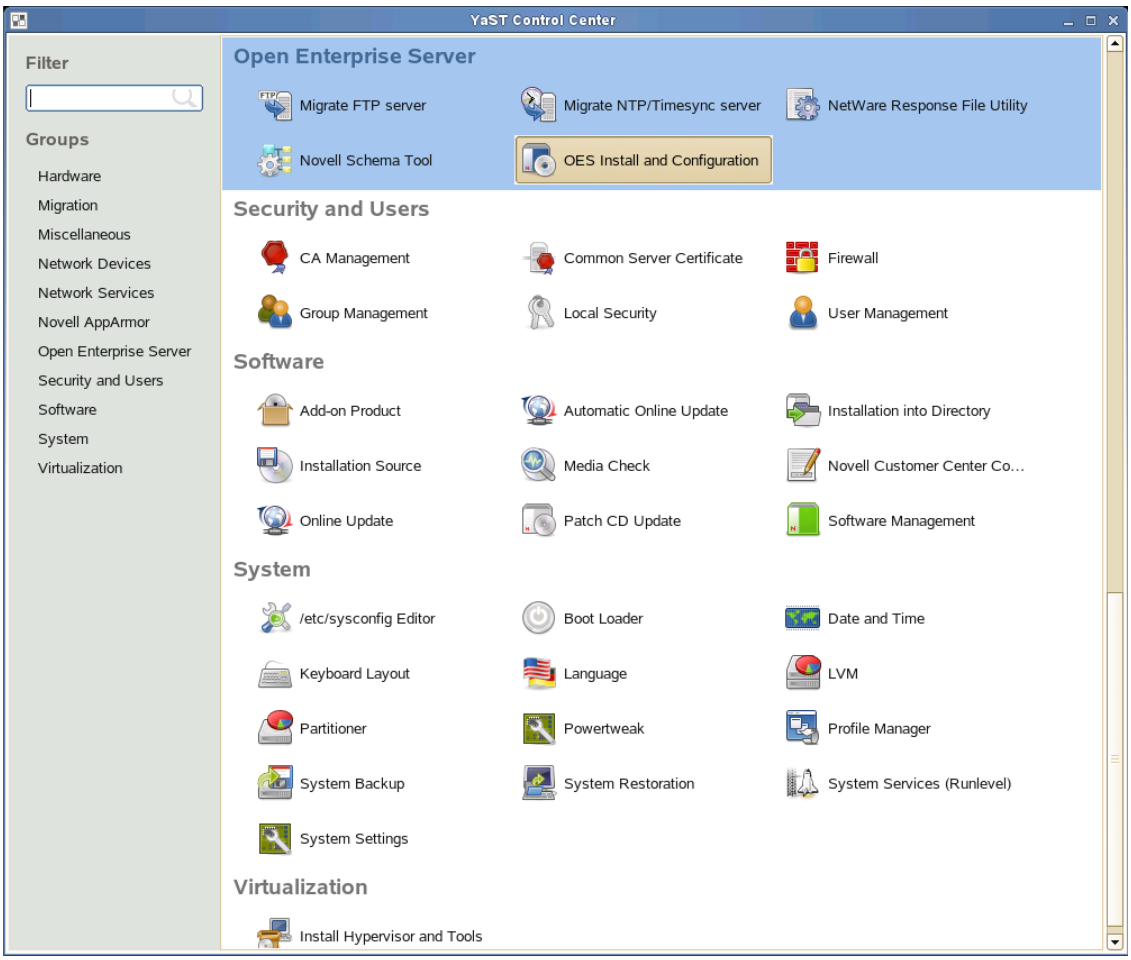
---

1. Before you begin, make sure your OES system setup meets the “Prerequisites and Guidelines” on page 45.
2. Open YaST2 using one of the following methods:
   - On your desktop, click the *YaST* shortcut icon to launch YaST, then enter the root password when prompted.
   - At a terminal, log in as the root user, then enter

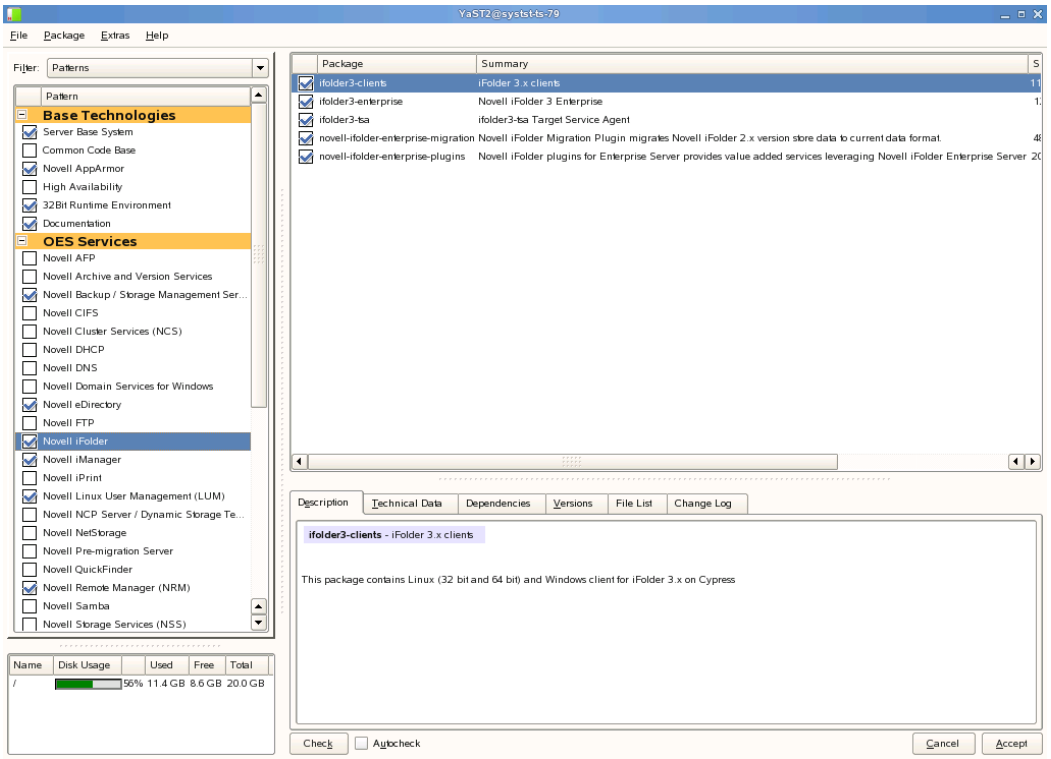
```
yast2
```

IMPORTANT: Ensure that you are logged in as the `root` user before performing the installation and configuration procedure.

3 In the left menu, select `Open Enterprise Server > OES Install and Configuration`.



A window displays with the Open Enterprise Server Services and Server Role patterns under software selection.



4 Select the *Novell iFolder* option.

You can install the iFolder Enterprise Server, Web Admin Server, and Web Access Server on the same computer or on different computers.

5 Click Details to resolve the dependency conflicts if you encounter any.

Resolve all the dependencies before continuing.

6 To begin the installation, click *Accept* at the bottom right of the screen.

7 When the installation is complete, either close YaST or continue with one or all of the following as needed:

- Section 6.2, “Deploying iFolder Server,” on page 51
- Section 6.3, “Configuring the iFolder Web Access Server,” on page 70
- Section 6.4, “Configuring the iFolder Web Admin Server,” on page 72

6.2 Deploying iFolder Server

This section describes how to configure Novell iFolder server in a Multi-server environment.

- Section 6.2.1, “Configuring the iFolder Enterprise Server,” on page 52
- Section 6.2.2, “Configuring the iFolder Slave Server,” on page 63
- Section 6.2.3, “Managing Server IP Change,” on page 70

6.2.1 Configuring the iFolder Enterprise Server

After you install the iFolder enterprise server, you must configure the iFolder services, including the LDAP, iFolder system, and iFolder administration settings.

1. If you plan to use an NSS volume as the System Store Path for the users' iFolder data, use iManager to create the NSS volume, then create a directory on the volume.

   For information, refer to "Managing NSS Volumes" in the *OES 2015: NSS File System Administration Guide for Linux*.

2. If you are using an NSS volume to store user data, you must set up NSS file system trustee rights for the Web server user object `wwwrun` before restarting your web server. At a terminal console prompt, log in as the root user or equivalent, then enter

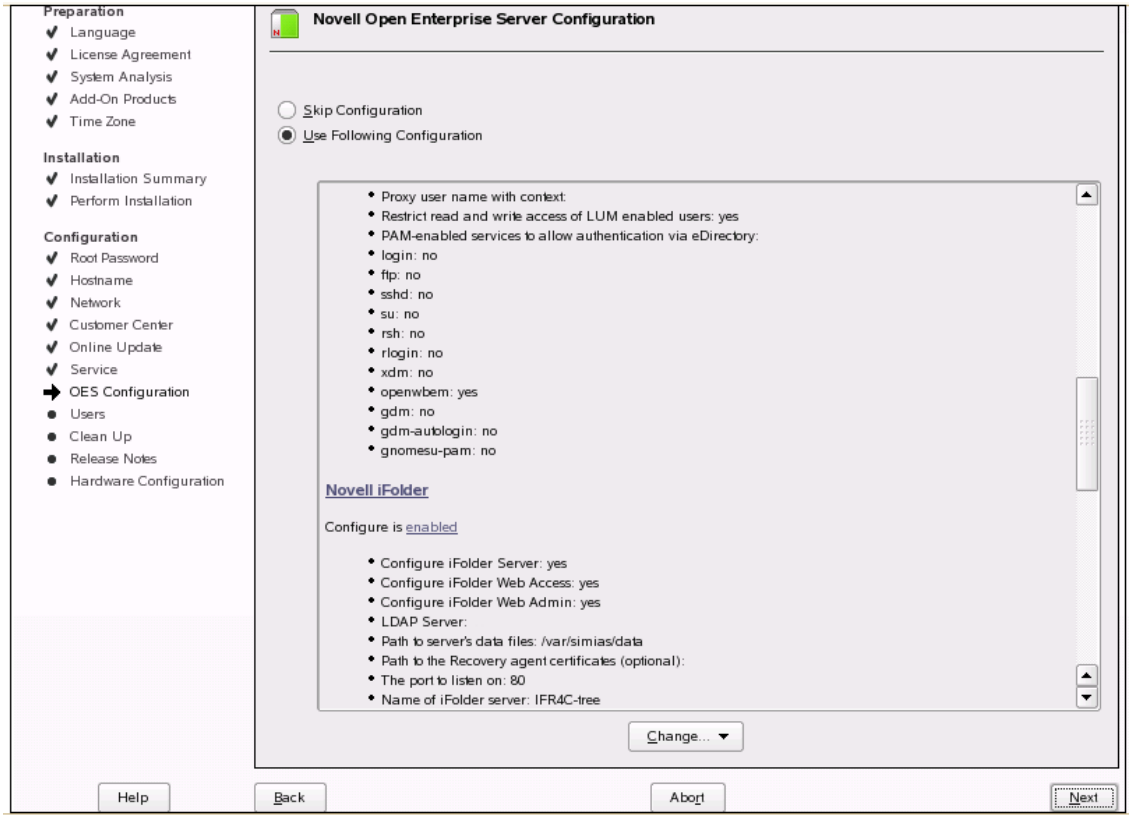
   ```
   rights -f /media/nss/NSSVOL/dirname -r rwfcem trustee wwwrun.ou.o.treename
   ```

   If you ever get, "`An Internal Error has occurred`" error message within the iManager plug-in, this is an indication that you have not set up file system trustee rights within NSS properly.

3. Log in to the server as the root user, or open a terminal console, enter `su`, then enter the `root` password.

4. Start YaST, follow the YaST on-screen instruction to finish the installation. For more information see Step 1 on page 49 through Step 7 on page 51 in the section Section 6.1, "Installing iFolder on an Existing OES Server," on page 49.

5. Select *Use Following Configuration* and click *Novell iFolder* to change the default configuration settings for iFolder.

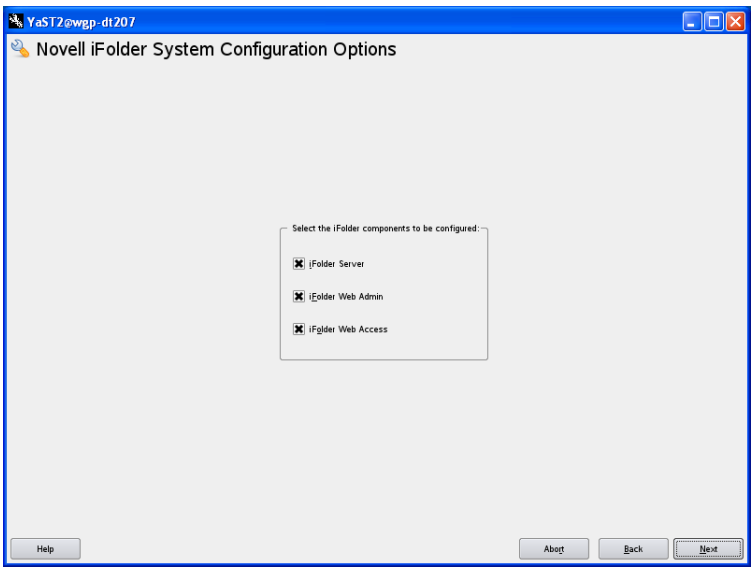


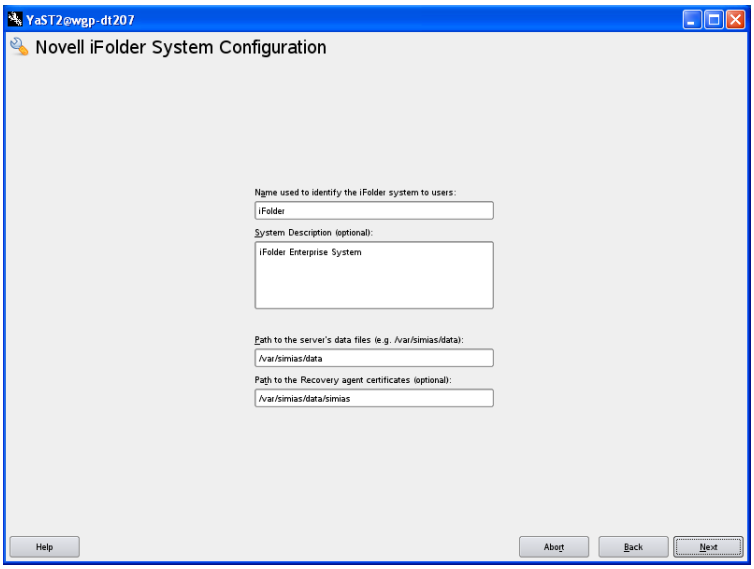
If you decide to use default settings, click *Next* to start Novell iFolder 3 configuration.

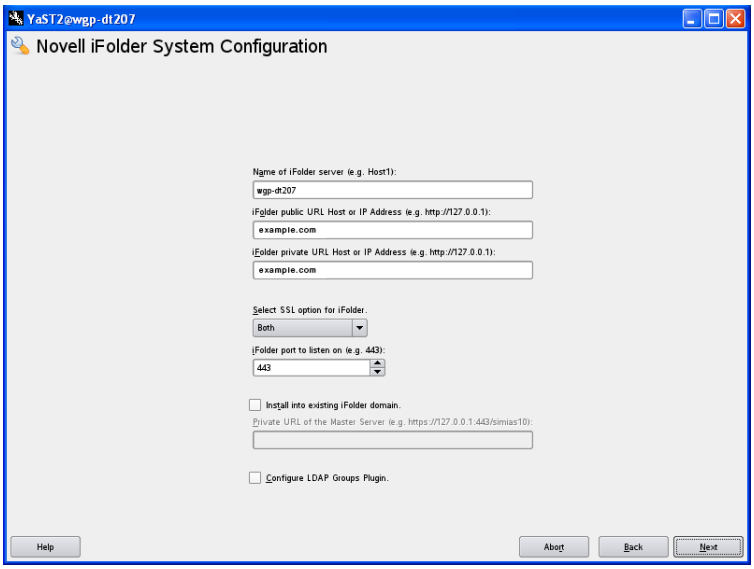
IMPORTANT: For security reasons, it is recommended that you always change the default iFolder configuration settings.

6 Follow the YaST on-screen instructions to proceed through the Novell iFolder 3 configuration. The following table summarizes the decisions you make.

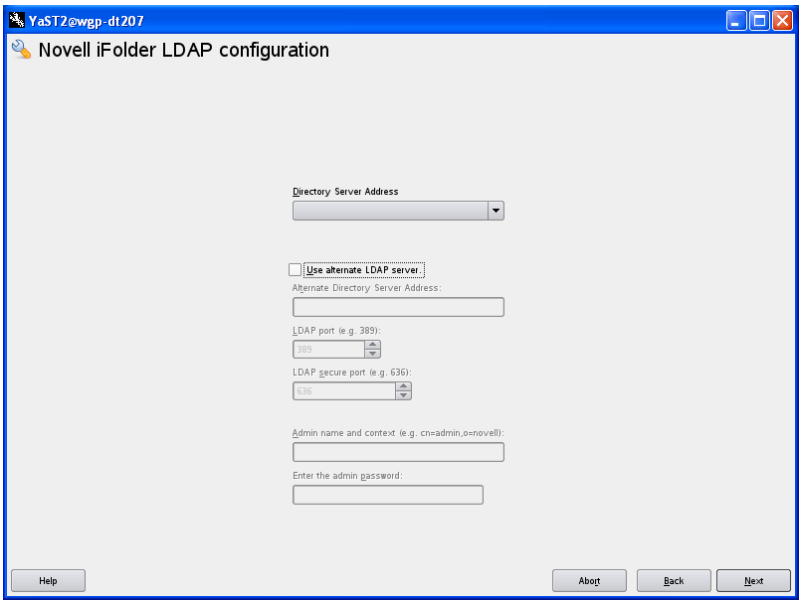
TIP: If the iFolder configuration failed at any stage, refer to the `/var/log/YaST2/y2log` file to find the details on the failure that help you in analyzing and troubleshooting the issues.

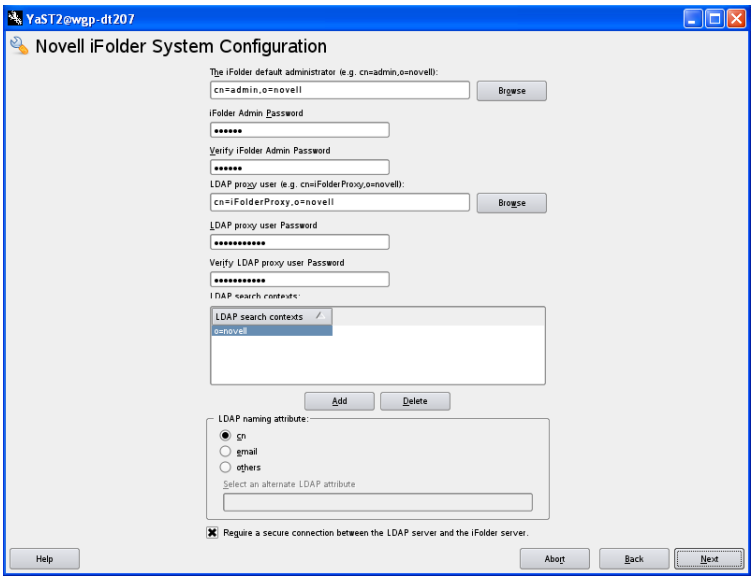
Install Settings	Description
iFolder components	 ◆ **Select the iFolder components to be configured:** Select the components you want to configure. You can choose any combination of iFolder components from the given options. The corresponding screens are displayed depending on your selection. ◆ **iFolder Server (optional):** Select the check box adjacent to the iFolder Server to configure iFolder server.This option lets you configure the settings for the iFolder server. It is the central repository for storing user iFolders and synchronizing files for enterprise users. ◆ **iFolder Web Admin (optional):** Select the check box adjacent to the iFolder Web Admin to configure iFolder Web Admin server. This option lets you create and configure settings for the Administrator user. The iFolder Admin user is the primary administrator of the iFolder Enterprise Server. The Web Admin server does not need to be configured on the iFolder Enterprise Server. Devoting a separate server to the Web Admin application improves the performance of the iFolder Enterprise Server by reducing the admin traffic. ◆ **iFolder Web Access (optional):** Select the check box adjacent to the iFolder Web Access to configure iFolder Web Access server. This option lets you configure the Web Access server, which is an interface that lets users have remote access to iFolders on the enterprise server. The Web Access server lets users perform all the operations equivalent to those of the iFolder client through using a standard Web browser. The Web Access server does not need to be configured in the same iFolder Enterprise Server. Channeling the user tasks to a separate server and thereby reducing the HTTP requests helps to improve the performance of the iFolder Enterprise Server.

Install Settings	Description
Novell iFolder System Configuration	 ◆ **Name Used to Identify the iFolder System to Users:** A unique name to identify your iFolder 3 server. For example, `iFolder Server`. ◆ **System Description:** A descriptive label for your iFolder 3 server. For example, `iFolder3 Enterprise Server` ◆ **Path to the Server Data File:** Specify the case-sensitive address of the location where the iFolder enterprise server stores iFolder application files as well as the users' iFolders and files. For example, `/var/simias/data/simias`. This location cannot be modified after install. ◆ **Path to the Recovery Agent Certificates (optional):** Specify the path to the recovery agent certificates that are used for recovering the encryption key. After you configure the path to the Recovery Agent, you must load the Agent certificates to this location. For more information, see Section 6.7, “Recovery Agent Certificates,” on page 87 . By default, eDirectory CA certificate is copied in this location with the name `sscert`. You can export the private key of this certificate using iManager. For information, see Section 6.7.6, “Exporting eDirectory CA Certificate Using iManager,” on page 94

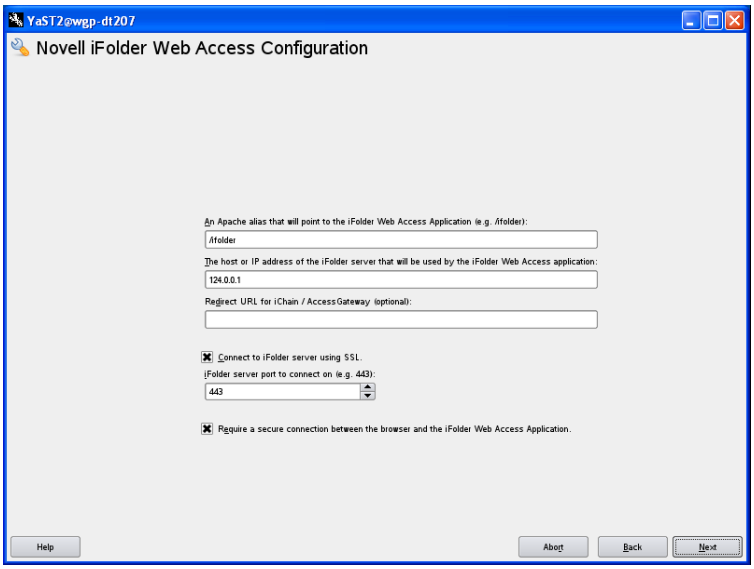
Install Settings	Description
Novell iFolder System Configuration	 ◆ **Name of iFolder Server:** Specify a unique name to identify your iFolder server. For example, `IF3EastS` ◆ **iFolder public URL Host or IP Address:** Specify the public URL to reach the iFolder server. **IMPORTANT:** You must specify the DNS name of the server as *iFolder Public URL* to connect the client to the server using a DNS name. In this case, users need not remember all the IP addresses they are provisioned to. A single DNS name can map them to the respective server IP based on their location as in office or home. ◆ **iFolder private URLHost or IP Address:** Specify the private URL corresponding to the iFolder server to allow communication between the servers within the iFolder domain. The Private URL and the Public URL can be the same. **NOTE:** You can use a single URL for the iFolder server if it is accessed only inside the corporate firewall. If the server needs to be accessed outside the firewall, you must provide two different URLs: Private and Public. The private URL is used for server to server communication within the corporate firewall and this should not be exposed to outside of the firewall. The public URL is used for the iFolder clients that can communicate from outside the corporate firewall. The clients can be inside or outside of the firewall and based on this, you can use private or public URL, or use public URL all the time.

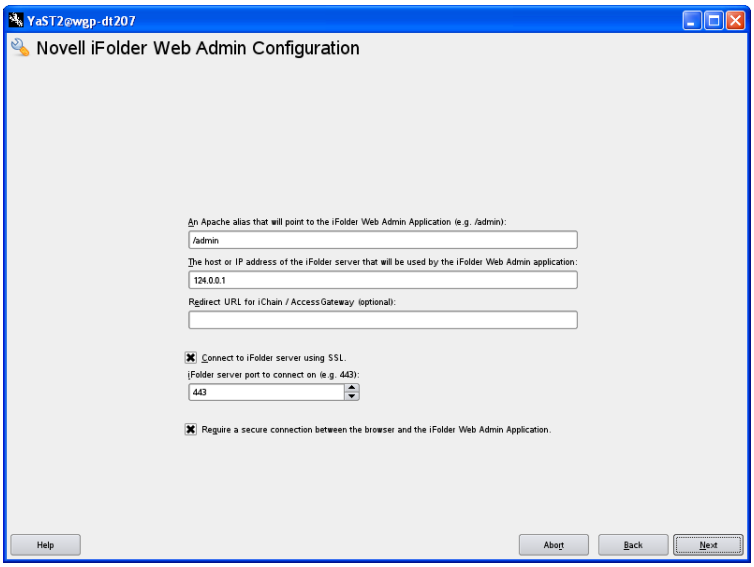
Install Settings	Description
Novell iFolder System Configuration	◆ **Configure SSL for iFolder:** There are three options to select from. ◆ **SSL:** Select *SSL* to enable a secure connection between the iFolder server, iFolder Web Admin server, iFolder Web Access server, and the iFolder clients. iFolder uses the HTTPS channel for communication. ◆ **Non SSL:** Select *Non SSL* to enable unsecured communication between the iFolder server, Web Admin server, Web Access server and the clients. iFolder uses the HTTP channel for communication. ◆ **Both:** This option is selected by default. Selecting *Both* enables you to select secure or non secure channel for communication between the iFolder server, Web Admin server, Web Access server and the clients. By default, these components use the HTTPS (secure) communication channel. However, all components can also be configured to use HTTP channel. ◆ **iFolder Port to Listen On:** Specify the port for the iFolder to Listen On. Port 443 is the default for SSL. ◆ **Install into Existing iFolder Domain:** If left unselected, this server becomes the Master iFolder server. Select this option when you want to use an existing iFolder domain and provide the Master server information. **IMPORTANT:** You must ensure that the server you install and the current iFolder domain are in the same LDAP tree. ◆ **Private URL of the Master Server:** Specify the private URL of the Master iFolder server that holds the master iFolder data for synchronization to the current iFolder Server. For example: https://127.0.1.1. For more information, see the Section 6.2.2, “Configuring the iFolder Slave Server,” on page 63 ◆ **Configure LDAP Groups plugin:** Select this option to configure the LDAP Groups plug-in. If this option is left unselected, iFolder will not have the LDAP Groups support enabled.

Install Settings	Description
Novell iFolder LDAP Configuration	 • **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add an alternate LDAP server (including Active Directory) to the list, you must specify the following values: • **Use alternate LDAP server:** Select this check box to specify an alternate LDAP server. On selecting this check box, the subsequent fields get enabled. • **Alternate Directory Server Address:** Specify the host or IP address of the alternate LDAP server that iFolder must use. • **LDAP port:** Specify the LDAP port to use for the alternate server. • **LDAP secure port:** Specify the LDAP secure port to use for the alternate server. • **Admin name and context:** Specify the administrator's full distinguished name for the alternate LDAP server. For example, `cn=LdapAdmin,o=acme`. • **Enter the admin password:** Enter the password for the alternate LDAP server. In case your directory server is a DSFW server, follow the steps given below to configure iFolder with DSFW server: 1. Select the *Use alternate LDAP server* check box. 2. Specify the IP address of the DSFW server in the *Alternate Directory Server Address* field. 3. Specify 1389 in the *LDAP port* field and 1636 in the *LDAP secure port* field. 4. Specify the eDirectory DN format and not DC context format in the *Admin name and context* field. 5. Enter the password in the *Enter the admin password* field.

Install Settings	Description
Novell iFolder System Configuration	 ◆ **The iFolder Default Administrator:** Specify the username for the default iFolder Admin user. Use the full distinguished name of the iFolder Admin user. For example:`cn=admin,o=acme`. ◆ **iFolder Admin Password:** Specify a password for the iFolder Admin user. ◆ **Verify iFolder Admin Password:** Type the password for the iFolder Admin user again. ◆ **LDAP Proxy User:** Specify the full distinguished name of the LDAP Proxy user. For example:`cn=iFolderproxy,o=acme`. You must ensure that the proxy user's context is present in the LDAP server. This means that for a proxy user cn=iFolderproxy,o=acme, the container o=acme must be present in the LDAP server. This user must have the Read right to the LDAP service. The LDAP Proxy user is used for provisioning the users between the iFolder Enterprise Server and the LDAP server. If the Proxy user does not exist, it is created and granted the Read right to the LDAP Search context(s). If the Proxy user already exists, it is granted the Read right to the LDAP Search context(s). If the Proxy user already exists, but the given credentials do not match, then a new Proxy user is automatically created. The Proxy user's domain name (dn) and password are stored by the iFolder. During eDirectory configuration, if you have selected the *Use Common Proxy User as default for OES Products* check box, then the proxy user and password fields are populated with common proxy user name and password. For more information on common proxy, refer to "Common Proxy User" in the *OES 2015: Planning and Implementation Guide*. **NOTE:** If you are using Active Directory or OpenLDAP as an LDAP source, you must not use common proxy.

Install Settings	Description
Novell iFolder System Configuration	◆ **LDAP Proxy User Password:** Specify a password for the LDAP Proxy user. By default, it is YaST-generated password. This field is disabled, if you have selected the *Use Common Proxy User as default for OES Products* check box during eDirectory configuration. **IMPORTANT:** You are recommended not to use this YaST-generated default password. You must specify the new proxy user password. ◆ **Verify LDAP Proxy User Password:** Type the password for the LDAP Proxy User again. ◆ **LDAP Search Context** Click *Add*, then specify an LDAP tree context to be searched for users and provisioning them in to iFolder. For example, `o=acme, o=acme2`, or `o=acme3`. You must ensure that the *LDAP Search Context* field does not remain empty. If the field is empty, the iFolder installation fails. You can modify the search context even after the configuration is complete by using the web admin console. For more information, see "Accessing and Viewing the Server Details Page" on page 160. **IMPORTANT:** You must ensure the following: ◆ The LDAP search context that you specify must be present in the LDAP server. If the LDAP search context is not present, the iFolder installation fails. ◆ In a multi-server setup, all the search contexts of the slave servers must be present in the master server as well. ◆ **LDAP Naming Attribute:** Select which LDAP attribute of the User account to apply when authenticating users. Each user enters a Username in this specified format at login time. Common Name (cn) is the default option. For example, if a user named John Smith has a common name of jsmith and e-mail of john.smith@example.com, this field determines whether the user enters jsmith or john.smith@example.com as the Username when logging in to the iFolder server. This setting cannot be changed after the install using the Web Admin console. If your directory server is configured with some other attribute as a unique login attribute for the users and you want to specify the same as login attribute for iFolder, then select the *others* option and specify the attribute name in the *Select an alternate LDAP attribute* field. ◆ **Require a secure connection between the LDAP server and the iFolder Server:** Select this option to establish a secure connection between the LDAP server and the iFolder server. This option is selected by default. If the LDAP server co-exists on the same machine as the iFolder server, an administrator can disable SSL, which increases the performance of LDAP authentications.

Install Settings	Description
iFolder Web Access Configuration	 ◆ **An Apache alias that will point to the iFolder Web Access Application:** Specify an Apache alias to point to the iFolder Web Admin application. This is an admin-friendly pointer for the Apache service. For example, /access ◆ **The host or IP address of the iFolder server that will be used by the iFolder Web Access application:** Specify the hostname or IP address of the iFolder Enterprise Server to be managed by the iFolder Web Admin application. The iFolder Web Admin application manages this host. ◆ **Connect to iFolder server using SSL:** This option is selected by default to establish a secure connection between iFolder enterprise server and the iFolder Web Access application. ◆ **iFolder server port to connect on:** Specify the port for the iFolder server to connect to the Web Access application. Port 443 is the default. Port 80 is the default value for non-SSL communication. ◆ **Require a secure connection between the browser and the iFolder Web Access application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.

Install Settings	Description
iFolder Web Admin Configuration	 ◆ **An Apache alias that will point to the iFolder Web Admin Application:** Specify the Apache alias to point to the iFolder Web Access Application. This is a user-friendly pointer for the Apache service. For example, /admin ◆ **The host or IP address of the iFolder server that will be used by the iFolder Web Admin application:** Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Access application. This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server. ◆ **Connect to iFolder server using SSL:** This option is selected by default to establish a secure connection between iFolder enterprise server and the iFolder Web Admin application. ◆ **iFolder server port to connect on:** Specify the port for the iFolder server to connect to the Web Admin application. Port 443 is the default. Port 80 is the default value for non-SSL communication. ◆ **Require a secure connection between the browser and the iFolder Web Admin application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two.

7 When the system prompts you to restart the Apache server, accept the option by clicking *Yes*, then restart the Apache server. This is necessary to use the new settings.

To manually restart the Apache Web server,

7a Open a terminal console, then log in as the `root` user.

7b Stop the Apache server by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 stop
```

```
rcapache2 stop
```

7c Start Apache by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 start
rcapache2 start
```

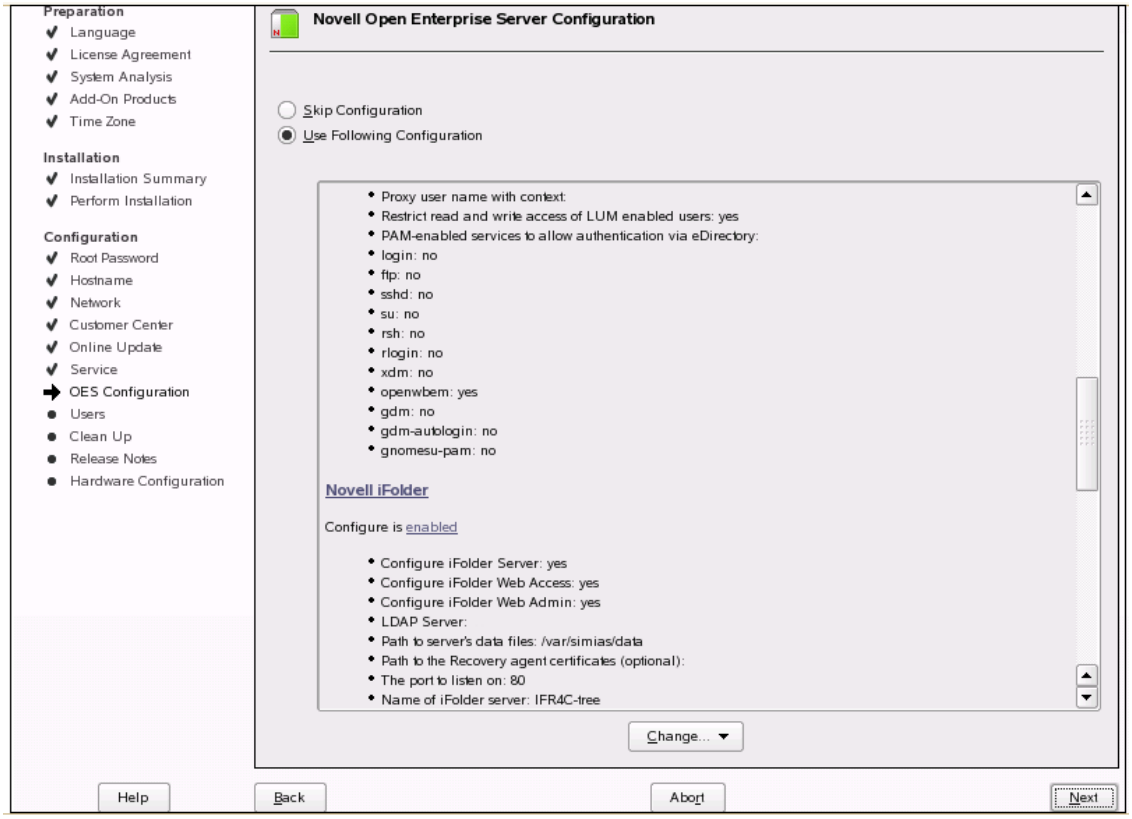
8 Go to Novell iManager to install the Novell iFolder plug-in or to manage iFolder services.

6.2.2 Configuring the iFolder Slave Server

To deploy iFolder server in a Multi-server set up,

After you configure the iFolder enterprise master server, you must configure the iFolder slave servers.

1 Select *Use Following Configuration* and click *Novell iFolder* in the window displayed.



2 Click *Novell iFolder* and then *Next* to start configuring the slave server.

IMPORTANT: For security reasons, it is recommended that you always change the default iFolder configuration settings.

3 Follow the YaST on-screen instructions to proceed through the Novell iFolder 3 configuration. The following table summarizes the decisions you make.

Install Settings	Description
iFolder components	◆ **Select the iFolder components to be configured:** Select the components you want to configure. You can choose any combination of iFolder components from the given options. The corresponding screens are displayed depending on your selection. ◆ **iFolder Server (optional):** Select the check box adjacent to the iFolder Server to configure iFolder server.This option lets you configure the settings for the iFolder server. It is the central repository for storing user iFolders and synchronizing files for enterprise users. ◆ **iFolder Web Admin (optional):** Select the check box adjacent to the iFolder Web Admin to configure iFolder Web Admin server. This option lets you create and configure settings for the Administrator user. The iFolder Admin user is the primary administrator of the iFolder Enterprise Server. The Web Admin server does not need to be configured on the iFolder Enterprise Server. Devoting a separate server to the Web Admin application improves the performance of the iFolder Enterprise Server by reducing the admin traffic. ◆ **iFolder Web Access (optional):** Select the check box adjacent to the iFolder Web Access to configure iFolder Web Access server. This option lets you configure the Web Access server, which is an interface that lets users have remote access to iFolders on the enterprise server. The Web Access server lets users perform all the operations equivalent to those of the iFolder client through using a standard Web browser. The Web Access server does not need to be configured in the same iFolder Enterprise Server. Channeling the user tasks to a separate server and thereby reducing the HTTP requests helps to improve the performance of the iFolder Enterprise Server.
Novell iFolder System Configuration	◆ **Name Used to Identify the iFolder System to Users:** A unique name to identify your iFolder 3 server. For example, `iFolder Server`. ◆ **System Description:** A descriptive label for your iFolder 3 server. For example, `iFolder3 Enterprise Server` ◆ **Path to the Server Data File:** Specify the case-sensitive address of the location where the iFolder enterprise server stores iFolder application files as well as the users' iFolders and files. For example, `/var/simias/data/simias`. This location cannot be modified after install. ◆ **Path to the Recovery Agent Certificates (optional):** Specify the path to the recovery agent certificates that are used for recovering the encryption key. If the path to the Recovery Agent is configured, you need to copy the Agent certificates to this location. For more information, see Section 6.7, “Recovery Agent Certificates,” on page 87.

Install Settings	Description

Novell iFolder System Configuration	◆ **Name of iFolder Server:** Specify a unique name to identify your iFolder server. For example, `IF3EastS`
	◆ **iFolder Public URL:** Specify the public URL to reach the iFolder server.
	◆ **iFolder Private URL:** Specify the private URL corresponding to the iFolder server to allow communication between the servers within the iFolder domain. The Private URL and the Public URL can be the same.
	◆ **Configure SSL for iFolder:** There are three options to select from.
	  ◆ **SSL:** Select *SSL* to enable a secure connection between the iFolder server, iFolder Web Admin server, iFolder Web Access server, and the iFolder clients. iFolder uses the HTTPS channel for communication.
	  ◆ **Non SSL:** Select *Non SSL* to enable unsecured communication between the iFolder server, Web Admin server, Web Access server and the clients. iFolder uses the HTTP channel for communication.
	  ◆ **Both:** This option is selected by default. Selecting *Both* enables you to select secure or non secure channel for communication between the iFolder server, Web Admin server, Web Access server and the clients. By default, these components use the HTTPS (secure) communication channel. However, all components can also be configured to use HTTP channel.
	◆ **iFolder Port to Listen On:** Specify the port for the iFolder to Listen On. Port 80 is the default
	◆ **Install into Existing iFolder Domain:** If left unselected, this server becomes the Master iFolder server. For slave server configuration, select this option.
	  ◆ **Private URL Host or IP address of the Master Server:** Specify the private URL of the Master iFolder server that holds the master iFolder data for synchronization to the current iFolder Server. For example: https://127.0.0.1:443/simias10.

Install Settings	Description
Novell iFolder LDAP Configuration	**IMPORTANT:** iFolder Master server and slave servers must be in the same eDirectory tree. ◆ **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add an alternate LDAP server (including Active Directory) to the list, you must specify the following values: ◆ **Use alternate LDAP server:** Select this check box to specify an alternate LDAP server. On selecting this check box, the subsequent fields get enabled. ◆ **Alternate Directory Server Address:** Specify the host or IP address of the alternate LDAP server that iFolder must use. ◆ **LDAP port:** Specify the LDAP port to use for the alternate server. ◆ **LDAP secure port:** Specify the LDAP secure port to use for the alternate server. ◆ **Admin name and context:** Specify the administrator's full distinguished name for the alternate LDAP server. For example, `cn=LdapAdmin,o=acme`. ◆ **Enter the admin password:** Enter the password for the alternate LDAP server. In case your directory server is a DSFW server, follow the steps given below to configure iFolder with DSFW server: 1. Select the *Use alternate LDAP server* check box. 2. Specify the IP address of the DSFW server in the *Alternate Directory Server Address* field. 3. Specify 1389 in the *LDAP port* field and 1636 in the *LDAP secure port* field. 4. Specify the eDirectory DN format and not DC context format in the *Admin name and context* field. 5. Enter the password in the *Enter the admin password* field.

Install Settings	Description
Novell iFolder System Configuration	◆ **The iFolder Default Administrator:** Specify the username for the default iFolder Admin user. Use the full distinguished name of the iFolder Admin user. For example:`cn=admin,o=acme` ◆ **iFolder Admin Password:** Specify a password for the iFolder Admin user. ◆ **Verify iFolder Admin Password:** Type the password for the iFolder Admin user again. ◆ **LDAP proxy User:** Specify the full distinguished name of the LDAP Proxy user. For example:cn=iFolderproxy,o=acme. This user must have the Read right to the LDAP service. The LDAP Proxy user is used for provisioning the users between the iFolder Enterprise Server and the LDAP server. If the Proxy user does not exist, it is created and granted the Read right to the LDAP Search context(s). If the Proxy user already exists, it is granted the Read right to the LDAP Search context(s). If the Proxy user already exists, but the given credentials dont match, then a new Proxy user is automatically created. The Proxy user's domain name (dn) and password are stored by the iFolder. During eDirectory configuration, if you have selected the *Use Common Proxy User as default for OES Products* check box, then the proxy user and password fields are populated with common proxy user name and password. **NOTE:** If you are using Active Directory or OpenLDAP as an LDAP source, you must not use common proxy. **NOTE:** *LDAP Proxy user* and *LDAP proxy user Password* options are disabled for all iFolder upgrade scenarios. For more information on Upgrade, see the *OES 2015: Migration Tool Administration Guide*. ◆ **LDAP proxy user Password:** Specify a password for the LDAP Proxy user. By default, it is YaST-generated password. This field is disabled, if you have selected the *Use Common Proxy User as default for OES Products* check box during eDirectory configuration **IMPORTANT:** You are recommended not to use this YaST-generated default password. You must specify the new proxy user password. ◆ **LDAP Search Context** Click *Add*, then specify an LDAP tree context to be searched for users and provisioning them in to iFolder. For example, `o=acme`, `o=acme2`, or `o=acme3`. You must ensure that the *LDAP Search Context* field does not remain empty. If the field is empty, the iFolder installation fails. You can modify the search context even after the configuration is complete by using the web admin console. For more information, see "Accessing and Viewing the Server Details Page" on page 160. The recommended settings must have a mutually exclusive LDAP search context list with other participating servers in the iFolder domain. **IMPORTANT:** Ensure that the LDAP search context you have specified is present in the LDAP server. If the LDAP search context is not present, the iFolder installation fails.

Install Settings	Description
Novell iFolder System Configuration	◆ **LDAP Naming Attribute:** Select which LDAP attribute of the User account to apply when authenticating users. Each user enters a Username in this specified format at login time. Common Name (cn) is the default and an e-mail address (e-mail) is the other option. For example, if a user named John Smith has a common name of jsmith and e-mail of john.smith@example.com, this field determines whether the user enters jsmith or john.smith@example.com as the Username when logging in to the iFolder server. This setting cannot be changed after the install. If your directory server is configured with some other attribute as a unique login attribute for the users and you want to specify the same as login attribute for iFolder, then select the *others* option and specify the attribute name in the *Select an alternate LDAP attribute* field. ◆ **Require a Secure Connection between the LDAP server and the iFolder Server:** Select this option to require a secure connection between the LDAP server and the iFolder server. This option is selected by default. If the LDAP server co-exists on the same machine as the iFolder server, an administrator can disable SSL, which increases the performance of LDAP authentications.
iFolder Web Access Configuration	◆ **An Apache alias that will point to the iFolder Web Access Application:** Specify an Apache alias to point to the iFolder Web Access application. This is an admin-friendly pointer for the Apache service. For example, /access ◆ **The host or IP address of the iFolder server that will be used by the iFolder Web Access application:** Specify the hostname or IP address of the iFolder Enterprise Server to be managed by the iFolder Web Access application. The iFolder Web Access application manages this host. ◆ **Redirect URL for iChain/AccessGateway (optional):** Specify the redirect URL for iChain/AccessGateway that will be used by the iFolder Web Access application. This URL is used for the proper logout of iChain/AccessGateway sessions along with the iFolder session. ◆ **Connect to iFolder server using SSL:** Select the check box to establish a secure connection between the iFolder enterprise server and the iFolder Web Admin application. ◆ **iFolder server port to connect on:** Specify the port for the iFolder server to connect to the Web Access application. Port 443 is the default for SSL. Port 80 is the default value for non-SSL communication. ◆ **Require a secure connection between the browser and the iFolder Web Access application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.

Install Settings	Description
iFolder Web Admin Configuration	◆ **An Apache alias that will point to the iFolder Web Admin Application:** Specify the Apache alias to point to the iFolder Web Admin Application. This is a user-friendly pointer for the Apache service. For example, /admin ◆ **The host or IP address of the iFolder server that will be used by the iFolder Web Admin application:** Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Admin application. This Web Admin application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server. ◆ **Redirect URL for iChain/AccessGateway (optional):** Specify the redirect URL for iChain/AccessGateway that will be used by the iFolder Web Access application. This URL is used for the proper logout of iChain/AccessGateway sessions along with the iFolder session. ◆ **Connect to iFolder server using SSL:** Select the check box to establish a secure connection between the iFolder enterprise server and the iFolder Web Admin application. ◆ **iFolder server port to connect on:** Specify the port for the Web Admin application to connect to the iFolder server. Port 443 is the default. Port 80 is the default value for non-SSL communication. ◆ **Require a secure connection between the browser and the iFolder Web Admin application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two.

4 Click *Accept* to complete the configuration.

5 When the system prompts you to restart the Apache server, accept the option by clicking *Yes*, then restart the Apache server. This is necessary to use the new settings.

To manually restart the Apache Web server,

5a Open a terminal console, then log in as the `root` user.

5b Stop the Apache server by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 stop
```

```
rcapache2 stop
```

5c Start Apache by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 start
```

```
rcapache2 start
```

6 Go to Novell iManager to install the Novell iFolder plug-in or to manage iFolder services.

7 If you are using an NSS volume to store user data, you must set up NSS file system trustee rights for the Web server user object `wwwrun` before restarting your web server. At a terminal console prompt, log in as the root user or equivalent, then enter

```
rights -f /media/nss/NSSVOL -r rwfcem trustee wwwrun.ou.o.treename
```

If you ever get `An Internal Error has occurred` error message within the iManager plug-in, this is a sure sign that you have not set up file system trustee rights within NSS properly.

6.2.3 Managing Server IP Change

When you change the Novell OES server IP address either through YaST or through command line, it does not automatically change the iFolder Service IP address. You can change the iFolder service IP address only by reconfiguring the iFolder service either through YaST or command line.

1. To change the IP address of an iFolder Enterprise server,
   - **1a** In the Web Admin console, click the Server tab and select the desired server.
     - **1a1** Change the Public URL and Private URL to reflect the new IP address and click *OK*.
     - **1a2** If the IP address change is for a master server, change the master URL for all the slave servers by using the *Server details* page of the respective slave servers listed in the *Server* page.

       For more information on this, see "Accessing and Viewing the Server Details Page" on page 160.
     - **1a3** If the LDAP server is configured to the same OES server, change the URL by using the *Server details* page.

       For more information on this, see "LDAP Server" on page 162.
2. To change the IP address of the Web Admin server,
   - **2a** In a terminal console, run the following command and change the iFolder enterprise server URL used by the Web Admin server application.

     ```
     /opt/novell/ifolder3/bin/ifolder-admin-setup
     ```

     For more information on this, see Section 6.4, "Configuring the iFolder Web Admin Server," on page 72.
3. To change the IP address of the Web Access server,
   - **3a** In a terminal console, run the following command and change the iFolder enterprise server URL used by the Web Access server application.

     ```
     /opt/novell/ifolder3/bin/ifolder-access-setup
     ```

     For more information on this, see Section 6.3, "Configuring the iFolder Web Access Server," on page 70.
4. Restart the system.

IMPORTANT: You must ensure that all the users whose iFolder clients are connected to the old server IP, are updated the client with the new IP address of the server. For more information on configuring server IP address in an iFolder client, see "Viewing and Modifying iFolder Account Settings" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

If the server is SSL enabled, you must ensure that the new SSL certificate is accepted by all the iFolder users.If a DNS name is used in the iFolder set-up and the new IP address uses the existing DNS name, then you don't need to change the DNS name for the client, instead accept the new certificate.

6.3 Configuring the iFolder Web Access Server

After you install the iFolder Web Access server, you must specify which iFolder enterprise server it supports and the user-friendly URL that users enter in their Web browsers to access it.

IMPORTANT: If you install iFolder when you install OES, the same parameters described in this procedure are available as an integrated part of the server install.

6.3.1 Configuring Web Access

1. Log in as the root user, or open a terminal console, enter `su`, then enter a password to log in as root.
2. Start YaST to refresh its list of installed configuration modules.
3. Click *Novell iFolder* in the window displays with Novell Open Enterprise Server Configuration.
4. Select *iFolder Web Access*.
5. Follow the YaST on-screen instructions to proceed through the iFolder 3 Web Access configuration. The table summarizes the decisions you make.

Install Settings	Description
Web Access Alias	The user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server. For example: `/ifolder`
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Access application. This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server.
Redirect URL for iChain/ AccessGateway	Specify the redirect URL for iChain/AccessGateway that will be used by the iFolder Web Access application. This URL is used for the proper logout of iChain/AccessGateway sessions along with the iFolder session.
Connect to iFolder server using SSL	Select the check box to establish a secure connection between the iFolder enterprise server and the iFolder Web Access application.
iFolder server port to connect on	Specify the port for the Web Admin application to connect to the iFolder server. Port 443 is the default. Port 80 is the default value for non-SSL communication.
Require SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.

6. When the system prompts you to restart the Apache server, accept the option by clicking *Yes*.

   Restarting Apache is necessary to use the new settings.

6.3.2 Configuring iFolder Web Access for iChain or AccessGateway

iFolder is interoperable with iChain and AccessGateway. iChain and AccessGateway requires its own session (user authentication data) logout which is provided by a specified URL. You must configure this URL for the Web Access console for proper logout of iChain/AccessGateway sessions along with iFolder.

1. Log in as the root user, or open a terminal console, enter `su`, then enter a password to log in as root.
2. Change the directory by typing `cd /opt/novell/ifolder3/bin` at the command prompt.
3. Run `ifolder-web-setup`.
4. Follow the on-screen instructions to proceed through the iFolder 3 Web Access configuration. The table summarizes the decisions you make.

Install Settings	Description
Web Access Alias	The user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server. For example: `/ifolder`
Require SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Access application. This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server.
Redirect URL	Specify the redirect URL for iChain or AccessGateway. This URL is used for the proper logout of iFolder Web Access console and iChain or AccessGateway sessions.
Require Server SSL	Skip this option to apply the default value.

5. When the system prompts you to restart the Apache server, accept the option by clicking *Yes*.

6.4 Configuring the iFolder Web Admin Server

After you install the iFolder Web Admin server, you must specify which iFolder enterprise server it supports and the user-friendly URL that users enter in their Web browsers to access it.

IMPORTANT: If you install iFolder with OES, the same parameters described in this procedure are available as an integrated part of the server install.

6.4.1 Configuring Web Admin Console

1. Log in as the root user, or open a terminal console, enter `su`, then enter a password to log in as root.
2. Start YaST to refresh its list of installed configuration modules.
3. Click *Novell iFolder* in the window displays with Novell Open Enterprise Server Configuration.
4. Click *Next* to start configuring the iFolder Web Admin.
5. In YaST, select *iFolder Web Admin*.
6. Follow the YaST on-screen instructions to proceed through the iFolder 3 Web Admin configuration. The table summarizes the decisions you make.

Install Settings	Description
Web Admin Alias	The user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server. For example: `/admin`
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Admin application. This Web Admin application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server.
Redirect URL for iChain/ AccessGateway	Specify the redirect URL for iChain/AccessGateway that will be used by the iFolder Web Access application. This URL is used for the proper logout of iChain/AccessGateway sessions along with the iFolder session.
Connect to iFolder server using SSL	Select the check box to establish a secure connection between the iFolder enterprise server and the iFolder Web Admin application.
iFolder server port to connect on	Specify the port for the Web Admin application to connect to the iFolder server. Port 443 is the default. Port 80 is the default value for non-SSL communication.
Require Server SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two. **IMPORTANT:** If this option is not enabled, you cannot login to Web Admin via iManager.

After you complete the YaST configuration for Web Admin console, restart Apache server.

7. When the system prompts you to restart the Apache server, accept the option by clicking *Yes*.

   Restarting Apache is necessary to use the new settings.

6.4.2 Configuring iFolder Web Admin for iChain or AccessGateway

iFolder is interoperable with iChain and AccessGateway. iChain and AccessGateway requires its own session (user authentication data) logout which is provided by a specified URL. You must configure this URL for the Web Admin console for proper logout of iChain/AccessGateway sessions along with iFolder.

1. Log in as the root user, or open a terminal console, enter `su`, then enter a password to log in as root.
2. Change the directory by typing `cd /opt/novell/ifolder3/bin` at the command prompt.
3. Run ifolder-admin-setup.
4. Follow the on-screen instructions to proceed through the iFolder 3 Web Admin configuration. The table summarizes the decisions you make.

Install Settings	Description
Web Admin Alias	The user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server. For example: `/ifolder`
Require SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two.
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Admin application. This Web Admin application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server.
Redirect URL	Specify the redirect URL for iChain or AccessGateway. This URL is used for the proper logout of iFolder Web Admin console and iChain or AccessGateway sessions.
Require Server SSL	Skip this option to apply the default value.

5. When the system prompts you to restart the Apache server, accept the option by clicking *Yes*.

6.5 Configuring the iFolder Enterprise Server with Active Directory as an LDAP source

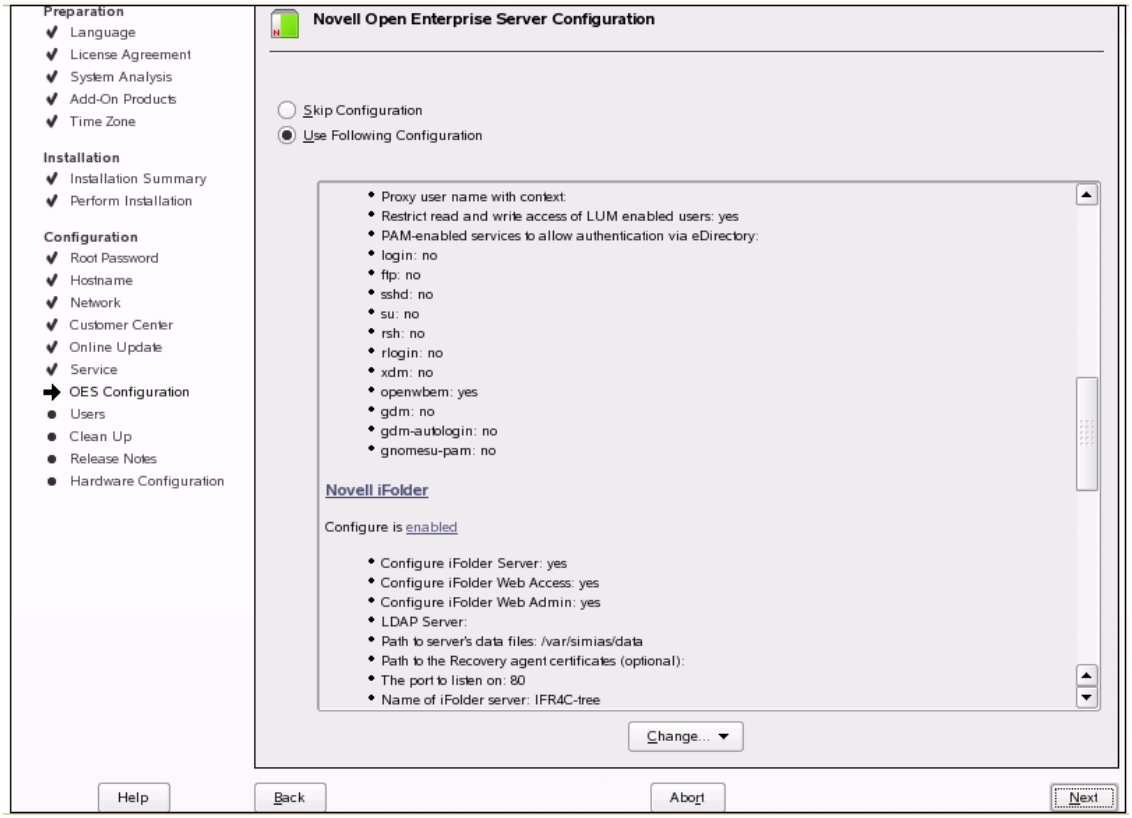
This section describes the steps to configure iFolder with Active Directory as an LDAP source. Before proceeding with the configuration, review Active Directory guidelines in the section Section 5.4, “Active Directory,” on page 46.

1. If you plan to use an NSS volume as the System Store Path for the users’ iFolder data, use iManager to create the NSS volume, then create a directory on the volume.

   For information, refer to “Managing NSS Volumes” in the *OES 2015: NSS File System Administration Guide for Linux*.
2. Log in to the server as the root user, or open a terminal console, enter `su`, then enter the `root` password.

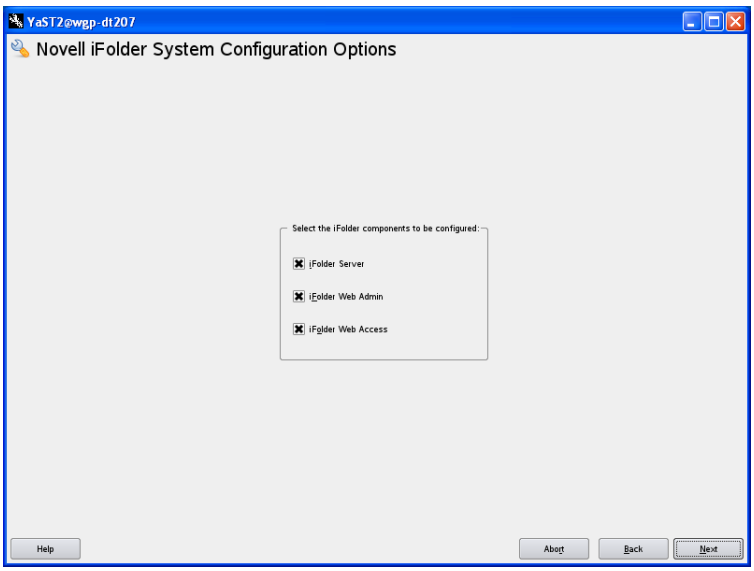
3 Start YaST, follow the YaST on-screen instructions to finish the installation. For more information see Step 1 on page 49 through Step 7 on page 51 in the section Section 6.1, “Installing iFolder on an Existing OES Server,” on page 49.

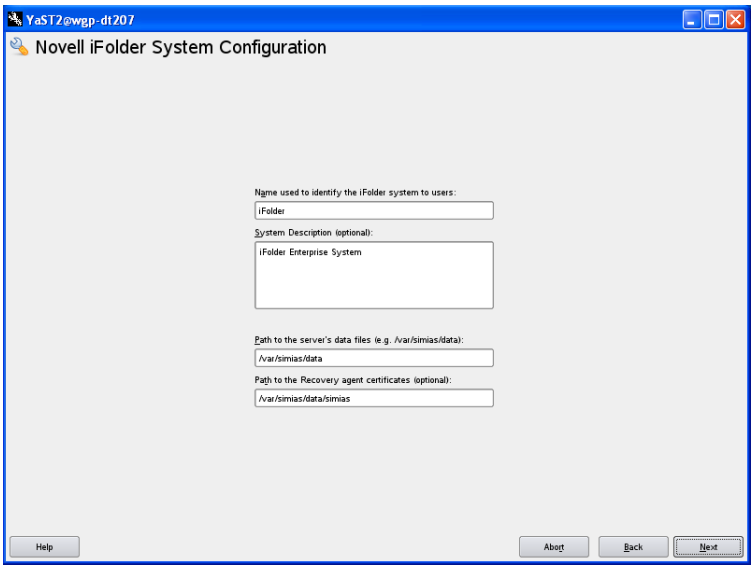
4 Select *Use Following Configuration* and click *Novell iFolder* to change the default configuration settings for iFolder.

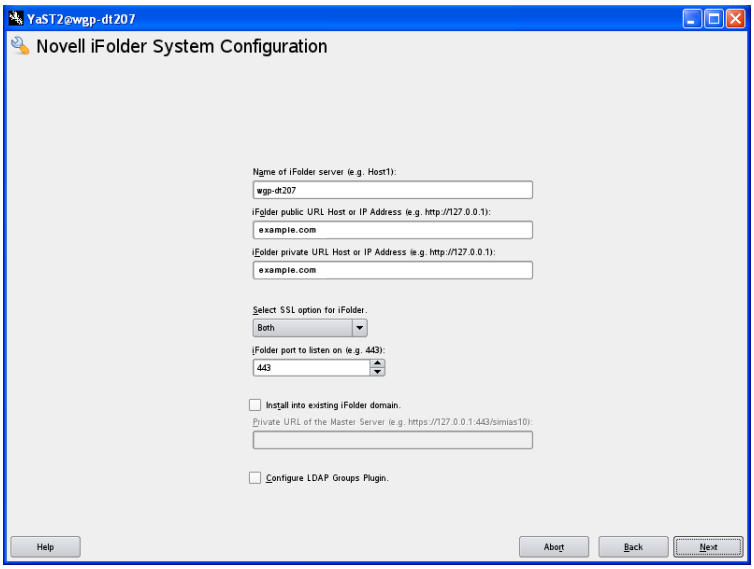


5 Follow the YaST on-screen instructions to proceed through the Novell iFolder 3 configuration. The following table summarizes the decisions you make.

TIP: If the iFolder configuration fails at any stage, refer to the `/var/log/YaST2/y2log` file to analyze and troubleshoot the issues.

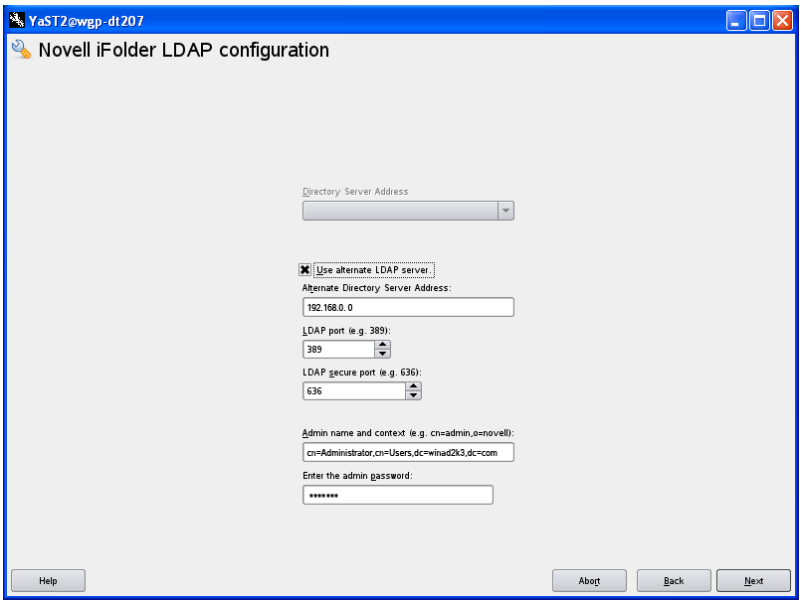
Settings	Description
iFolder components	 ◆ **Select the iFolder components to be configured:** Select the components you want to configure. You can choose any combination of iFolder components from the given options. The corresponding screens are displayed depending on your selection. ◆ **iFolder Server:** Select the iFolder Server check box to configure iFolder server.This option lets you configure the settings for the iFolder server. It is the central repository for storing user iFolders and synchronizing files for enterprise users. ◆ **iFolder Web Admin (optional):** Select the iFolder Web Admin check box to configure the iFolder Web Admin server. This option lets you create and configure settings for the Administrator user. The iFolder Admin user is the primary administrator of the iFolder Enterprise Server. The Web Admin server does not need to be configured on the iFolder Enterprise Server. Devoting a separate server to the Web Admin application improves the performance of the iFolder Enterprise Server by reducing the admin traffic. ◆ **iFolder Web Access (optional):** Select the iFolder Web Access check box to configure iFolder Web Access server. This option lets you configure the Web Access server, which is an interface that lets users have remote access to iFolders on the enterprise server. The Web Access server lets users perform all the operations equivalent to those of the iFolder client using a standard Web browser. The Web Access server does not need to be configured on the same iFolder Enterprise Server. Channeling the user tasks to a separate server and thereby reducing the HTTP requests helps to improve the performance of the iFolder Enterprise Server.

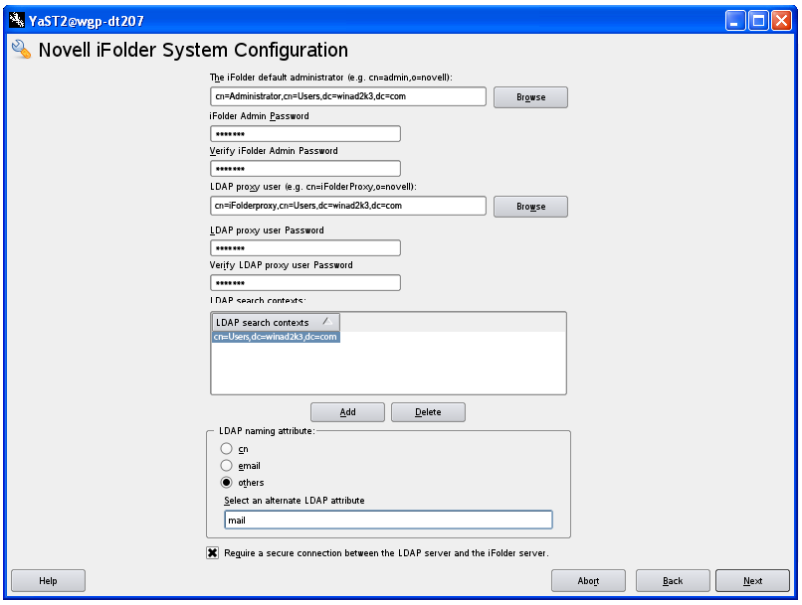
Settings	Description
Novell iFolder System Configuration	 ◆ **Name Used to Identify the iFolder System to Users:** A unique name to identify your iFolder 3 server. For example, `iFolder Server`. ◆ **System Description:** A descriptive label for your iFolder 3 server. For example, `iFolder3 Enterprise Server` ◆ **Path to the Server Data File:** Specify the case-sensitive address of the location where the iFolder enterprise server stores iFolder application files as well as the users' iFolders and files. For example, `/var/simias/data/simias`. This location cannot be modified after install. ◆ **Path to the Recovery Agent Certificates (optional):** Specify the path to the recovery agent certificates that are used for recovering the encryption key. After you configure the path to the Recovery Agent, you must load the Agent certificates to this location. For more information, see Section 6.7, “Recovery Agent Certificates,” on page 87 . By default, eDirectory CA certificate is copied in this location with the name `sscert`. You can export the private key of this certificate using iManager. For informtaion, see Section 6.7.6, “Exporting eDirectory CA Certificate Using iManager,” on page 94.

Settings	Description
Novell iFolder System Configuration	 ◆ **Name of iFolder Server:** Specify a unique name to identify your iFolder server. For example, `IF3EastS` ◆ **iFolder public URL Host or IP Address:** Specify the public URL to reach the iFolder server. **IMPORTANT:** You must specify the DNS name of the server as *iFolder Public URL* to connect the client to the server using a DNS name. In this case, users need not remember all the IP addresses they are provisioned to. A single DNS name can map them to the respective server IP based on their location as in office or home. ◆ **iFolder private URLHost or IP Address:** Specify the private URL corresponding to the iFolder server to allow communication between the servers within the iFolder domain. The Private URL and the Public URL can be the same. **NOTE:** You can use a single URL for the iFolder server if it is accessed only inside the corporate firewall. If the server needs to be accessed outside the firewall, you must provide two different URLs: Private and Public. The private URL is used for server to server communication within the corporate firewall and this should not be exposed to outside of the firewall. The public URL is used for the iFolder clients that can communicate from outside the corporate firewall. The clients can be inside or outside of the firewall and based on this, you can use private or public URL, or use public URL all the time.

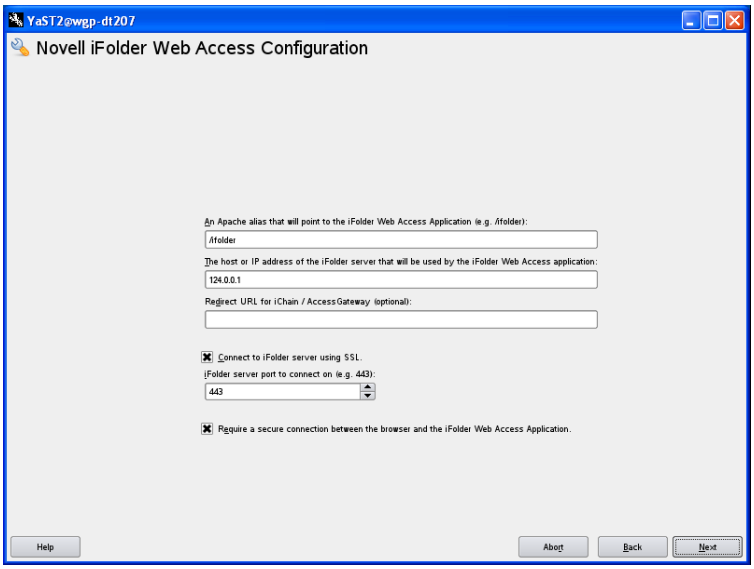
Settings	Description

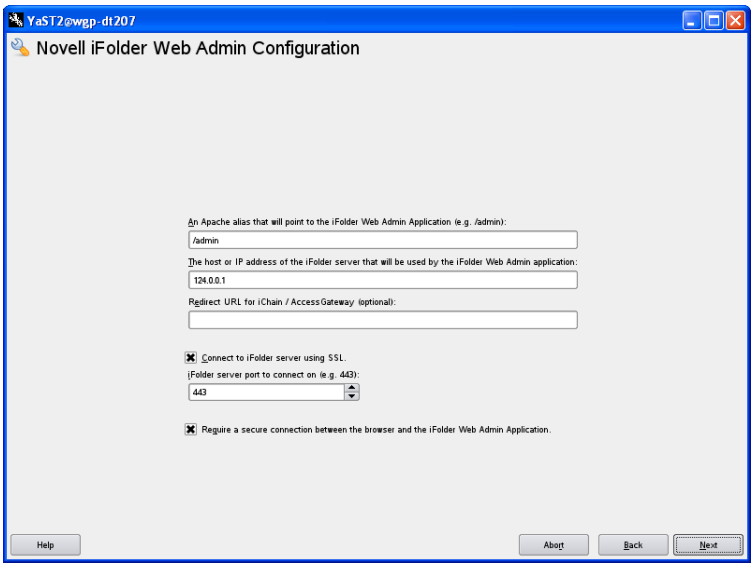
Novell iFolder System Configuration	◆ **Configure SSL for iFolder:** There are three options to select from.
	  ◆ **SSL:** Select *SSL* to enable a secure connection between the iFolder server, iFolder Web Admin server, iFolder Web Access server, and the iFolder clients. On selecting this option, iFolder uses the HTTPS channel for communication.
	  ◆ **Non SSL:** Select *Non SSL* to enable unsecured communication between the iFolder server, Web Admin server, Web Access server and the clients. On selecting this option, iFolder uses the HTTP channel for communication.
	  ◆ **Both:** This option is selected by default. Selecting *Both* enables you to select secure or non secure channel for communication between the iFolder server, Web Admin server, Web Access server and the clients. By default, these components use the HTTPS (secure) communication channel. However, all components can also be configured to use the HTTP channel.
	◆ **iFolder Port to Listen On:** Specify the port for the iFolder to Listen On. Port 443 is the default for SSL.
	◆ **Install into Existing iFolder Domain:** If left unselected, this server becomes the Master iFolder server. Select this option when you want to use an existing iFolder domain and provide the Master server information.
	IMPORTANT: You must ensure that the server you install and the current iFolder domain are in the same LDAP tree.
	  ◆ **Private URL of the Master Server:** Specify the private URL of the Master iFolder server that holds the master iFolder data for synchronization to the current iFolder Server. For example: https://127.0.1.1. For more information, see the Section 6.2.2, “Configuring the iFolder Slave Server,” on page 63.
	◆ **Configure LDAP Groups plugin:** Select this option to configure the LDAP Groups plug-in. If this option is left unselected, iFolder will not have the LDAP Groups support enabled.

Settings	Description
Novell iFolder LDAP Configuration	 ◆ **Use alternate LDAP server:** To use Active Directory as an LDAP source, select this check box. On selecting this check box, the subsequent fields get enabled. ◆ **Alternate Directory Server Address:** Specify the host or IP address of the Active Directory server that iFolder must use. ◆ **LDAP port:** Specify the LDAP port to use for the alternate server. ◆ **LDAP secure port:** Specify the LDAP secure port to use for the alternate server. ◆ **Admin name and context:** Specify the full distinguished name of the LDAP administrator for the Active Directory server. For example, cn=Administrator,cn=Users,dc=winad2k3,dc=com. You must ensure that the LDAP administrator has admin rights for the user container (for example, cn=Administrator,cn=Users,dc=winad2k3,dc=com). This is required because iFolder creates iFolder admin and iFolder proxy user objects under this container. The administrator must also have admin rights to the schema naming context (for example, cn=Schema,cn=Configuration,dc=winad2k3,dc=com). This is required as iFolder extends user object schema ◆ **Enter the admin password:** Enter the password of the LDAP admin of the Active Directory server.

Settings	Description
Novell iFolder System Configuration	 ◆ **The iFolder Default Administrator:** Specify the username for the default iFolder Admin user. Use the full distinguished name of the iFolder Admin user. For example, cn=Administrator,cn=Users,dc=winad2k3,dc=com. **NOTE:** The iFolder default administrator and the LDAP administrator need not be the same. iFolder does not require admin rights for iFolder admin user in Active Directory. ◆ **iFolder Admin Password:** Specify a password for the iFolder Admin user. ◆ **Verify iFolder Admin Password:** Type the password for the iFolder Admin user again. ◆ **LDAP Proxy User:** Specify the full distinguished name of the LDAP Proxy user. For example: cn=iFolderproxy,cn=Users, dc=winad2k3,dc=com. The LDAP Proxy user is used for provisioning the users between the iFolder Enterprise Server and the LDAP server. If the Proxy user does not exist, it is created. However, you must ensure that the iFolder proxy user has read permissions to all user containers configured and attributes of user objects.

Settings	Description
Novell iFolder System Configuration	◆ **LDAP Proxy User Password:** Specify a password for the LDAP Proxy user. You must ensure that the password that you specify conforms to the Active Directory password policy guidelines. ◆ **Verify LDAP Proxy User Password:** Type the password for the LDAP Proxy User again. ◆ **LDAP Search Context** Click *Add*, then specify an LDAP tree context to be searched for users that are to be provisioned to iFolder. For example, cn=Users,dc=winad2k3,dc=com. You must ensure that the *LDAP Search Context* field does not remain empty. If the field is empty, the iFolder installation fails. You can modify the search context even after the configuration is complete by using the web admin console. For more information, see "Accessing and Viewing the Server Details Page" on page 160. **IMPORTANT:** You must ensure the following: ◆ The LDAP search context that you specify must be present in the LDAP server. If the LDAP search context is not present, the iFolder installation fails. ◆ In a multi-server setup, all the search contexts of the slave servers must be present in the master server as well. ◆ You must ensure that the search context that you specify is a user container. ◆ If you specify multiple search contexts, you must ensure that the iFolder proxy user has read permissions for all those contexts/ containers and attributes of all the user objects under those containers. ◆ **LDAP Naming Attribute:** Specify which LDAP attribute of the User account to apply when authenticating users. Each user enters a Username in this specified format at login time. To set mail as an LDAP naming attribute, you must select the *others* option and specify mail in the *Select an alternate LDAP attribute* field. Similarly, you can set sAMAccountName as the LDAP naming attribute. ◆ **Require a secure connection between the LDAP server and the iFolder Server:** Select this option to establish a secure connection between the LDAP server and the iFolder server. This option is selected by default. If the LDAP server co-exists on the same machine as the iFolder server, an administrator can disable SSL, which increases the performance of LDAP authentications.

Settings	Description
iFolder Web Access Configuration	 ◆ **An Apache alias that will point to the iFolder Web Access Application:** Specify an Apache alias to point to the iFolder Web Access application. This is an admin-friendly pointer for the Apache service. For example, /access ◆ **The host or IP address of the iFolder server that will be used by the iFolder Web Access application:** Specify the hostname or IP address of the iFolder Enterprise Server to be used by the iFolder Web Access application. This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server ◆ **Connect to iFolder server using SSL:** This option is selected by default to establish a secure connection between iFolder enterprise server and the iFolder Web Access application. ◆ **iFolder server port to connect on:** Specify the port for the iFolder server to connect to the Web Access application. Port 443 is the default. Port 80 is the default value for non-SSL communication. ◆ **Require a secure connection between the browser and the iFolder Web Access application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.

Settings	Description
iFolder Web Admin Configuration	 ◆ **An Apache alias that will point to the iFolder Web Admin Application:** Specify the Apache alias to point to the iFolder Web Admin Application. This is a user-friendly pointer for the Apache service. For example, /admin ◆ **The host or IP address of the iFolder server that will be used by the iFolder Web Admin application:** Specify the host or IP address of the iFolder Enterprise Server to be managed by the iFolder Web Admin application. ◆ **Connect to iFolder server using SSL:** This option is selected by default to establish a secure connection between iFolder enterprise server and the iFolder Web Admin application. ◆ **iFolder server port to connect on:** Specify the port for the iFolder server to connect to the Web Admin application. Port 443 is the default. Port 80 is the default value for non-SSL communication. ◆ **Require a secure connection between the browser and the iFolder Web Admin application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two.

6 When the system prompts you to restart the Apache server, accept the option by clicking *Yes*, then restart the Apache server. This is necessary to use the new settings.

To manually restart the Apache Web server,

6a Open a terminal console, then log in as the `root` user.

6b Stop the Apache server by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 stop
```

```
rcapache2 stop
```

6c Start Apache by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 start
```

```
rcapache2 start
```

7 Go to Novell iManager to install the Novell iFolder plug-in or to manage iFolder services.

8 If you are using an NSS volume to store user data, you must set up NSS file system trustee rights for the Web server user object `wwwrun` before restarting your web server. At a terminal console prompt, log in as the root user or equivalent, then enter

```
rights -f /media/nss/NSSVOL -r rwfcem trustee wwwrun.ou.o.treename
```

If you ever get `An Internal Error has occurred` error message within the iManager plug-in, this is a sure sign that you have not set up file system trustee rights within NSS properly.

6.6 Installing the Novell iFolder 3 Plug-In for iManager

Before you can manage Novell iFolder 3 services, you must install the iFolder iManager Module for Novell iManager 2.7. After it is installed, this plug-in is named Novell iFolder 3 in the iManager Roles and Tasks list.

Make sure you meet prerequisites, then use one of the methods for installing the iFolder plug-in:

- Section 6.6.1, “Prerequisites,” on page 85
- Section 6.6.2, “Installing a Plug-In When RBS Is Not Configured,” on page 85
- Section 6.6.3, “Installing a Plug-In When RBS Is Configured,” on page 86

6.6.1 Prerequisites

Novell iManager 2.7

If you have not already done so, install Novell iManager 2.7 on the same or different server as your iFolder server. For information, see *Novell iManager 2.7 Installation Guide* (http://www.novell.com/documentation/imanager27/)

Role-Based Services

The iFolder 3 plug-in supports the optional use of Role Based Services (RBS) in Novell iManager. RBS gives you the ability to assign specific tasks to iManager admin users and to present the admin user with only the tools necessary to perform a specified set of tasks or manage only objects as determined by their roles. What admin users see when they access iManager is based on their role assignments in eDirectory. Only the roles and tasks assigned to that user are displayed.

For information, see “Configuring Role-Based Services” (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a31aexm.html) in the *Novell eDirectory 8.8 Administration Guide* (http://www.novell.com/documentation/edir88/)

6.6.2 Installing a Plug-In When RBS Is Not Configured

If you do not have Role-Based Services (RBS) configured for eDirectory, install the iFolder Manager Module as follows:

1 In a Web browser, log in to iManager on the iFolder server where you installed iManager.

```
https://ifolder.example.com/nps/iManager.html
```

Replace *`ifolder.example.com`* with the IP address (such as `192.168.1.1`) or the DNS name of the iFolder server.

If you installed iManager on a different server in the same tree as your iFolder server, log in to iManager on that server.

2 In the toolbar, click the *Configure* icon (person seated behind a desk).

3 In Roles and Tasks, expand *Plug-in Installation*, then click *Available Novell Plug-In Modules*.

4 Locate the *iFolder iManager Module* plug-in, select its plug-in check box, then click *Install*.

This install takes a few minutes. You should receive a message confirming a successful install.

5 Click *OK* to dismiss the message, then close iManager.

6 Stop and start the Apache server by entering the following command at the terminal console:

```
/etc/init.d/apache2 restart
```

7 Verify that the plug-in is enabled by opening iManager in a Web browser and checking to see if the Novell iFolder 3 plug-in appears in the list of Roles and Tasks.

For information, see Section 6.8, “Accessing iManager and the Novell iFolder Web Admin,” on page 95.

8 Continue with Section 6.9, “Provisioning Users, Groups and iFolder Services,” on page 96.

6.6.3 Installing a Plug-In When RBS Is Configured

If you are running iManager in Assigned Mode and have RBS configured for eDirectory, complete the following steps to install the iFolder iManager Module.

IMPORTANT: To re-install an existing plug-in, you must first delete the rbsModule object for that plug-in from eDirectory, using the *Module Configuration* > *Delete RBS Module* task.

---

1 In a Web browser, log in to iManager as an RBS Collection Owner on the system where you installed iFolder.

```
https://ifolder.example.com/nps/iManager.html
```

Replace `ifolder.example.com` with the IP address (such as `192.168.1.1`) or the DNS name of the iFolder server.

2 In the toolbar, click the *Configure* icon (person seated behind a desk).

3 In Roles and Tasks, expand *Plug-in Installation*, then click *Available Novell Plug-In Modules*.

4 Locate the iFolder iManager Module, select its plug-in check box, then click *Install*.

This install takes a few minutes. You should receive a message confirming a successful install.

5 Click *OK* to dismiss the message, then close iManager.

6 Stop and start the Apache server by entering the following command at the terminal console:

```
/etc/init.d/apache2 restart
```

7 Click the *Configure* icon.

8 Under *Role-Based Services*, select *RBS Configuration*.

The table on the Collections tabbed page displays modules ready to update.

9 Locate the collection where you want to install the plug-in, then click its *Out-of-Date* number.

The *iFolder iManager Module* plug-in should be displayed under *Modules Not Yet Installed* column.

10 Select the *iFolder iManager Module* plug-in.

11 Click *Update*.

12 Wait for the Completed message, then click *OK* to continue.

13 Verify that the plug-in is enabled by opening iManager in a Web browser and checking to see if the Novell iFolder 3 plug-in appears in the list of *Roles and Tasks*.

For information, see Section 6.8, “Accessing iManager and the Novell iFolder Web Admin,” on page 95.

6.7 Recovery Agent Certificates

The Recovery agent is a trustworthy organization that issues and signs public key certificates. This organization should be an entity independent of entities owning the iFolder server's infrastructure, or, independent of the IT department if deployed in a corporate environment.

Recovery agent certificates are the public key certificates used for encrypting the data encryption key. The user selects one of these certificates to perform the data key encryption for later key recovery. The supported certificate formats are `*.cer` and `*.der(X.509)`.

You can also use self-signed certificates if iFolder is deployed in a trusted environment.The certificates are generated by using the YaST CA Management plug-in or OpenSSL tools.

- Section 6.7.1, “Understanding Digital Certification,” on page 87
- Section 6.7.2, “Creating a YaST-based CA,” on page 88
- Section 6.7.3, “Creating Self-Signed Certificates Using YaST,” on page 90
- Section 6.7.4, “Exporting Self-Signed Certificates,” on page 92
- Section 6.7.5, “Exporting Self-Signed Private Key Certificates For Key Recovery,” on page 93
- Section 6.7.6, “Exporting eDirectory CA Certificate Using iManager,” on page 94
- Section 6.7.7, “Using KeyRecovery to Recover the Data,” on page 94
- Section 6.7.8, “Managing Certificate Change,” on page 95

6.7.1 Understanding Digital Certification

To protect user data from access by unauthorized people, the user data is encrypted by using keys that always occur in private and public key pairs. The keys are applied to the user data in a mathematical process, producing an altered data record in which the original content can no longer be identified.

Private Key: The private key must be kept safely by the key owner. Accidental publication of the private key compromises the key pair and can also be a security threat. The private key is either held by the Recovery agent or the user.

Public Key: The key owner circulates the public key for use by third parties.

Certified Authority (CA): The public key process is popular and there are many public keys in circulation. Certified Authorities are the trustworthy organizations that issue and sign public key certificates. The CA ensures that a public key actually belongs to the assumed owner. The certificates that a CA holds contain the name of the key owner, the corresponding public key, and the electronic signature of the person or entity issuing the certificate. The iFolder Recovery Agents are examples of one kind of CA.

Public Key Infrastructure (PKI): Certificate authorities are usually part of a certification infrastructure that is also responsible for the other aspects of certificate management, such as publication, withdrawal, and renewal of certificates. An infrastructure of this kind is generally referred to as a Public Key Infrastructure or PKI. One familiar PKI is the X.509 Public Key Infrastructure

(PKIX). The security of such a PKI depends on the trustworthiness of the CA certificates. To make certification practices clear to PKI customers, the PKI operator defines a certification practice statement (CPS) that defines the procedures for certificate management. This should ensure that the PKI issues only trustworthy certificates.

X.509 Public Key Infrastructure: The X.509 Public Key Infrastructure is defined by the IETF (Internet Engineering Task Force) that serves as a model for almost all publicly-used PKIs today. In this model, authentication is made by certificate authorities (CA) in a hierarchical tree structure. The root of the tree is the root CA, which certifies all sub-CAs. The lowest level of sub-CAs issue user certificates. The user certificates are trustworthy by certification that can be traced to the root CA.

X.509 Certificate: An X.509 certificate is a data structure with several fixed fields and, optionally, additional extensions. The fixed fields mainly contain the name of the key owner, the public key, and the data such as name and signature relating to the issuing CA. For security reasons, a certificate should only have a limited period of validity, so a field is also provided for this date. The CA guarantees the validity of the certificate in the specified period. The CPS usually requires the issuing CA to create and distribute a new certificate before expiration. The extensions can contain any additional information. An application is only required to be able to evaluate an extension if it is identified as critical. If an application does not recognize a critical extension, it must reject the certificate. Some extensions are only useful for a specific application, such as signature or encryption.

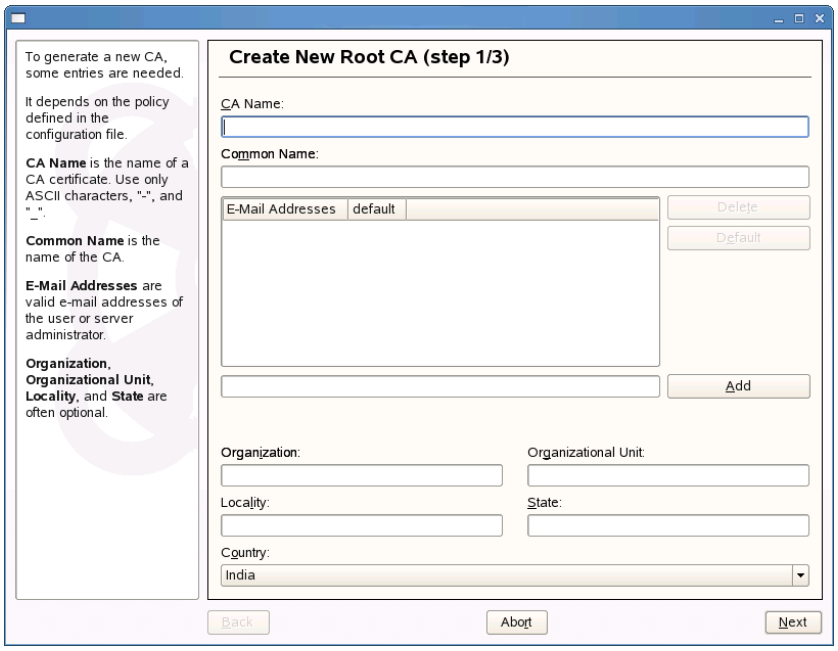
Table 6-1 *X.509v3 Certificate*

Field	Content
Version	The version of the certificate, for example, v3
Serial Number	Unique certificate ID (an integer)
Signature	The ID of the algorithm used to sign the certificate
Issuer	Unique name (DN) of the issuing authority (CA)
Validity	Period of validity
Subjectr	Unique name (DN) of the owner
Subject Public Key Info	InfoPublic key of the owner and the ID of the algorithm
Issuer Unique ID	Unique ID of the issuing CA (optional)
Subject Unique ID	Unique ID of the owner (optional)
Extensions	Optional additional information, such as KeyUsage or BasicConstraints

YaST-Based PKI: YaST contains modules for the basic management of X.509 certificates. This mainly involves the creation of CAs and their certificate. YaST provides tools for creating and distributing CAs and certificates, but cannot currently offer the background infrastructure that allow continuous update of certificates and CRLs. To set up a small PKI, you can use the available YaST modules. However, you should use commercial products to set up an official or commercial PKI.

6.7.2 Creating a YaST-based CA

1. Start YaST and go to *Security and Users* > *CA Management*.
2. Click *Create Root CA*.



3 Enter the information for creating the CA in the dialog boxes. The following table summarizes the decisions you make.

CA Settings	Description
CA Name	Enter the technical name of the CA. Because the Directory names, among other things, are derived from this name, you must use only the characters listed in the help. The technical name is also displayed in the overview when the module is started.
Common Name	Enter the name of the CA.
E-Mail Address	You can enter several e-mail addresses that a CA user can see. This is helpful for inquiries.
Country	Select the country where the CA is operated.
Organization, Organizational Unit, Locality, State	Optional Values.

4 Click *Next*.

5 Enter a password in the second dialog. This password is always required when using the CA for generating certificates. The following table summarizes the decisions you make.

CA Settings	Descriptions
Password	Specify a password with a minimum length of five characters. To confirm, re-enter it in the next field.
Key Length (bit)	Select the key length. You can choose a value between a minimum of 512 and a maximum of 2048.

CA Settings	Descriptions
Valid Period (days)	The Valid Period in the case of a CA defaults to 3650 days (roughly ten years). This long period makes sense because the replacement of a deleted CA involves an enormous administrative effort.
Advanced Options	Advanced Options are very special options. **WARNING:** If you change these options, iFolder cannot guarantee that the generated certificate works correctly. Clicking Advanced Options opens a dialog for setting different attributes from the X.509 extensions. These values have rational default settings and should only be changed if you are really sure of what you are doing.

YaST displays the current settings for confirmation.

6 Click *Create*.

The root CA is created then appears in the overview.

6.7.3 Creating Self-Signed Certificates Using YaST

iFolder key recovery mechanism uses the X509 certificates to manage the keys. You can either get a certificate from an external Certified Authority, for instance Verisign or generate a self-signed certificate if deployed in a trusted environment, where a trusted user-admin relationship exists.

NOTE: In certificates intended for e-mail signature, the e-mail address of the sender (the private key owner) should be contained in the certificate to enable the e-mail program to assign the correct certificate. For certificate assignment during encryption, it is necessary for the e-mail address of the recipient (the public key owner) to be included in the certificate. In the case of server and client certificates, the hostname of the server must be entered in the Common Name field. The default validity period for certificates is 365 days.

This section discusses creating self-signed certificates for encryption and self-signed key certificate for key recovery using YaST.

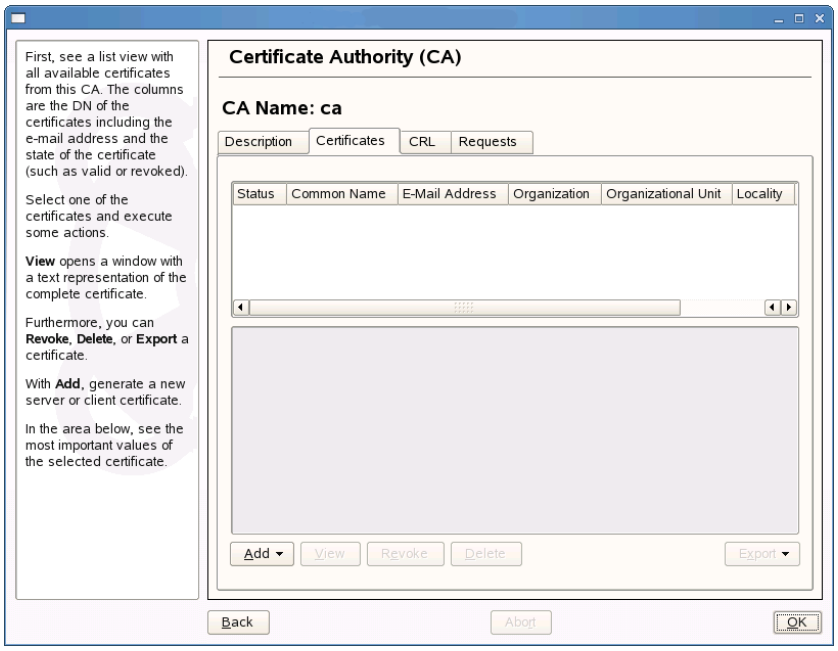
1 Start YaST and go to *Security and Users* > *CA Management*.

2 Select the required CA and click *Enter CA*.

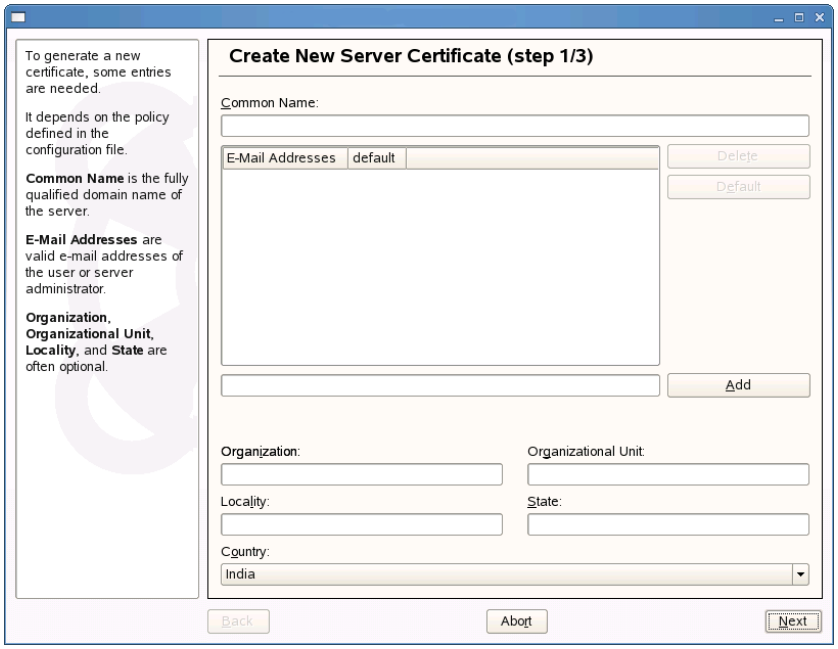
3 Enter the password for the CA if asked for.

YaST displays the CA key information in the Description tab.

4 Click Certificates tab.



5 Click *Add* > *Add Server Certificate*.



6 Enter the information for creating the certificates in the dialog boxes. The following table summarizes the decisions you make.

CA Settings	Description
Common Name	Enter the name of the CA.
E-Mail Address	You can enter several e-mail addresses that a CA user can see. This is helpful for inquiries.
Country	Select the country where the CA is operated.
Organization, Organizational Unit, Locality, State	Optional Values.

7 Enter a password in the second dialog.The following table summarizes the decisions you make.

CA Settings	Descriptions
Password	Specify a password with a minimum length of five characters. To confirm, re-enter it in the next field.
Key Length (bit)	Select the key length of minimum value of 512 and a maximum value of 2048. iFolder supports only 512, 1024 and 2048 as the key length.
Valid Period (days)	The Valid Period in the case of a CA defaults to 3650 days (roughly ten years). This long period makes sense because the replacement of a deleted CA involves an enormous administrative effort.
Advanced Options	Advanced Options are very special options. **WARNING:** If you change these options, iFolder cannot guarantee that the generated certificate works correctly. Clicking Advanced Options opens a dialog for setting different attributes from the X.509 extensions. These values have rational default settings and should only be changed if you are really sure of what you are doing.

YaST displays the current settings for confirmation.

For information on encryption, see "Encryption" in the *Novell iFolder 3.9.2 Cross-Platform User Guide* and "Using the Recovery Agent" in the *Novell iFolder 3.9.2 Security Administration Guide*.

6.7.4 Exporting Self-Signed Certificates

1 Click Export drop-down and select *Export to File*.

2 Select *Only the Certificate in PEM format*.

3 Specify a password of minimum length of five characters.

4 Click *Browse* to find a location to save the file, then specify a filename for the certificate you have created.

5 Click *OK* to save the certificate.

6 Convert the certificate in PEM format to DER format using OpenSSL command as given below:

```
openssl x509 -in <certificate>.pem -inform PEM -out <certificate>.der -outform
DER
```

7 Copy the certificate in DER format to the location you have configured for loading Recovery Agent Certificate during iFolder configuration.

If the certificate is expired, you need to load the new certificates again to this location.

8 Restart the iFolder server to load the Recovery agent certificates.

6.7.5 Exporting Self-Signed Private Key Certificates For Key Recovery

1 Click Export drop-down and select *Export to File*.

2 Select *Certificate and the Key in PKCS12 Format*.

3 Specify a new password and re-enter that for confirmation.

This password is used with the certificate and the keys exported to a file in XML format.

IMPORTANT: You must use a password different from the one you have used for certificate creation.

4 Specify a filename for the certificate you have created and click Browse to find a location to save the file.

5 Click *OK* to save the certificate.

6.7.6 Exporting eDirectory CA Certificate Using iManager

1 Login to iManager using iManager administrator credentials.

2 Click *Novell Certificate Server* > *Configure Certificate Authority*.

3 Click the *Certificates* tab.

4 Select the Root CA and click *Export*.

5 Select the organizational CA from the Certificates list and click *Next* to export the file in pfx format.

6.7.7 Using KeyRecovery to Recover the Data

Each iFolder has a unique data encryption key which is auto-generated during iFolder creation. The key is encrypted by using a passphrase provided by the user and also by using the public key with the Recovery agent. If the users forget the passphrase, they cannot access the iFolder data and they must reset the passphrase to gain access to the iFolder data.

Users can reset the passphrase by launching the Passphrase Recovery Wizard using the *Security* > *Forgot Passphrase* option in the client. If the user does not have the secret file or the new data file, then they can use the wizard to export the old data file and then e-mail the file to the administrator. The administrator can then use the KeyRecovery tool to generate the new data file and send it back to the user. The KeyRecovery tool can be downloaded from the iFolder 3 Welcome page.

NOTE: The keys are exported to a file in XML format. It is recommended to save the file as `<filename>.xml`

This section help you understand the process followed by a Recovery agent to retrieve the key.

1 Download the Passphrase Recovery Tool from the iFolder 3 Welcome page. For Linux and Macintosh, run `KeyRecovery` and for Windows run `KeyRecovery.exe` and follow the on-screen instructions.

The following table summarizes the decisions you make.

Parameters	Description
Encrypted Key file path	Specify the path (including the file name of the encrypted key) for reading the encrypted keys.
Private Key	Specify the path to the private key file (PKCS12 file format, *.p12).
Decrypted Key file path	Specify the path to store the decrypted key file. Ensure that the filename also included in the path you specify.
Private Key password	Specify the password to decrypt the private key.

Parameters	Description
Encrypt Result key	Specify whether you want to encrypt the decrypted key with one time passphrase. Default value: Yes
One time passphrase	Specify a one time passphrase to encrypt the decrypted keys.

2 Send the decrypted key usually by replying to the mail attached with the encrypted keys and the one-time passphrase (if the key is encrypted using the one-time passphrase) to the user.

3 Send the one-time passphrase (if the key is encrypted using the one-time passphrase) to the user through any other communication channel other than the one you used to exchange the key files.

6.7.8 Managing Certificate Change

The self-signed certificates for iFolder services change when they are expired, revoked, or replaced with a new certificate by a new CA.

Client: When a new certificate is created, the user has to approve of from the client side. The client prompts for the new certificate for the user to accept it.

Web Admin Server: The change in the certificate is not automatically communicated to the Web Admin server. You must reconfigure the Web Admin server for the new certificate to be accepted. By default, the new certificate is accepted in the server side. In the front-end, the browser is updated automatically when the server is updated with the new certificate.

Web Access Server: The change in the certificate is not automatically communicated to the Web Admin server. You must reconfigure the Web Access server for the new certificate to be accepted. By default, the new certificate is accepted in the server side. In the front-end, the browser is updated automatically when the server is updated with the new certificate.

6.8 Accessing iManager and the Novell iFolder Web Admin

The Novell iFolder Web Admin is the tool used to manage your iFolder server.

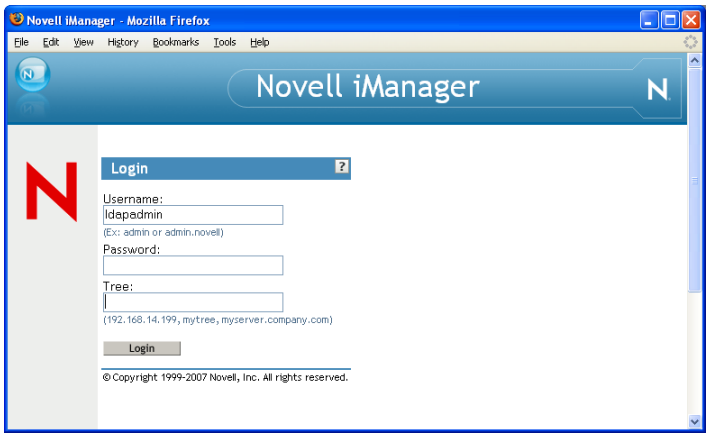
1 Open a Web browser to the iManager Login page by entering the following location:

`http://servername.example.com/nps/iManager.html`

Replace *`servername.example.com`* with the DNS name or IP address (such as `192.168.1.1`) of the OES server where you installed iManager. This might be the same or different computer where you installed iFolder 3.9 server or iFolder 3.9 Web Admin console.

2 (Conditional) If prompted to accept the server's certificate, review the certificate information, then click *OK* to accept it if it is valid.

3 On the iManager Login page, specify the Admin username and password you created during the OES install, then click *Login*.



The user name can be specified as contextless (such as *admin*) or with the context (such as `cn=admin.o=acme`). You must use a dot delimiter in fully distinguished names when working in iManager.

The iManager Web management interface opens with *Roles and Tasks* listed in the navigator on the left.

4 In Roles and Tasks, click *iFolder 3.9* > *Launch Admin Console*.

5 Specify the DNS name or IP address of the iFolder enterprise server you want to manage.

For example, type `svr1.example.com or 192.168.1.1`.

6 Do one of the following:

6a If you logged in to iManager with the same username as the iFolder Admin user of the Web Admin, select Authenticate Using Current iManager Credentials.

6b If you logged in to iManager with a different username than the iFolder Admin user of the Web Admin, leave the check box Authenticate Using Current iManager Credentials unselected, then specify the iFolder Admin username and password.

7 Click *OK*.

IMPORTANT: If you are logged in to iManager with iManager admin credential, iFolder Web Admin does not ask the credentials again for logging into Web Admin console.

For information, see Section 11.2, “Connecting to the iFolder Server,” on page 147.

Novell iFolder opens to the User page, which consists of a tabbed list of the main administrative functions that can be performed on iFolder domain.

6.9 Provisioning Users, Groups and iFolder Services

After you configure your Novell iFolder enterprise server, you must specify containers and groups as Search DNs in the LDAP settings. iFolder uses these to provision user and group accounts. You can provision users and iFolders through iFolder Web Admin console. For more information, see the following:

- Chapter 11, “Managing iFolder Services via Web Admin,” on page 147
- Chapter 12, “Managing iFolder Users,” on page 169
- Chapter 13, “Managing iFolders,” on page 177

6.9.1 Prerequisites

- "Users and LDAP Contexts" on page 97
- "Extending LDAP User Objects for iFolder 3.9" on page 97

Users and LDAP Contexts

The contexts you plan to use as LDAP Search DNs in the LDAP settings must exist in the LDAP directory; they are not created and configured from within the iFolder plug-in.

For information about configuring user, group, and container objects, see the *Novell eDirectory 8.8 Administration Guide* (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a2iii88.html).

Extending LDAP User Objects for iFolder 3.9

To enable LDAP attribute-based provisioning, you must Extend the LDAP user schema with the i*FolderUserProvision* auxiliary object class with *iFolderHomeServer* as one attribute. For Active Directory, you must use Active Directory tools to extend User Objects with *iFolderHomeServer* as an attribute.

1. Login to iManager using iManager administrator credentials.
2. Click *View Objects* icon to open the Object view.
3. Browse and find the appropriate tree where the desired users are listed.

   For more information on this, see the *Novell iManager 2.7 Administration Guide (http://www.novell.com/documentation/imanager27/)*.
4. Click the desired user object you want to extend, and open the *Action* window, then click *Object Extensions*.
5. Click *OK* in the right-side panel that displays the object extensions detail.
6. In the new page that lists the current auxiliary class extensions, click *Add.*
7. From the pop-up window, select *iFolderUserProvision* entry, and click *OK*.
8. Click *Close*.

   For more information on this, see the section Roles and Tasks (http://www.novell.com/documentation/imanager27/imanager_admin_274/?page=/documentation/imanager27/imanager_admin_274/data/b8im2s7.html) in the *iManager Administration Guide*.
9. To add *iFolderHomeServer* attribute, click the same object to pop-up the *Tasks* window.
10. Select *Modify Objects* to display the object modification details in the right panel.
11. Under the *General* tab in that page, click the *Other* link, and select *iFolderHomeServer* from the *Unvalued Attribute* list, then click the arrow mark.
12. In the pop-up window, provide a value for the *iFolderHomeServer* attribute and click *OK*.

    The value can either be the IP address or the DNS name of the iFolder server assigned to this user.
13. click *Apply* to save the modifications.
14. For all the users, repeat the Step 1 thru Step 13 on page 97.

Command Line Option

You can also use the following script to extend the existing user objects or create a new user object with the `iFolderUserProvision` object class extension.

1. In the terminal console, type `/opt/novell/ifolder3/bin/iFolderLdapUserUpdate.sh`.
2. Type `./iFolderLdapUserUpdate.sh -h <Ldap URL> -d <admin DN> -w <admin password> -u <user DN> [-s <surname>] [-c <user password>] [-i <iFolder Home Server>]`.

   For example: `./iFolderLdapUserUpdate.sh -h ldaps://10.10.10.10 -d admin,o=novell -w secret -u cn=abc,o=novell -s xyz  -c secret -i 10.10.10.10`.

6.10 Distributing the iFolder Client to Users

After you configure iFolder services on the enterprise server, users can download the install files for the iFolder client from the OES 2015 Welcome page.

NOTE: iFolder does not support a silent install (that is, a scriptable non-interactive install) on any platform. A silent install is possible for the Linux client using its `.rpm` files, but it is not supported.

- Section 6.10.1, “Accessing the OES Welcome Page,” on page 98
- Section 6.10.2, “Downloading the iFolder Client,” on page 98
- Section 6.10.3, “Installing the iFolder Client,” on page 99

6.10.1 Accessing the OES Welcome Page

1. Open a Web browser to the following location to open the server’s Welcome page:

   `http://ifolder3.example.com`.

   Replace `ifolder3.example.com` with the DNS name or the IP address (such as `192.168.1.1`) of the OES server.

6.10.2 Downloading the iFolder Client

On the OES Welcome page, users can select one of the following client links from the *Client Software* page under *Available Downloads* to download the install files for the iFolder client for Novell iFolder 3.9.2:

Users can download the following install files:

Table 6-2 *Client Install Files*

Link Name	Operating System/Description	Filename
iFolder Client for Linux (SLED 10)	Suse Linux Enterprise Desktop 10	`ifolder3-linux.tar.gz`
iFolder Client for Linux (SLED 11)	Suse Linux Enterprise Desktop 11	`ifolder3-sled11.tar.gz`
Install script for iFolder Linux Client	Use the script to automatically install the iFolder client for Linux	`install-ifolder-script.sh`

Link Name	Operating System/Description	Filename
iFolder 32-bit Client for Windows	Windows XP SP3/Windows 7	`ifolder3-windows.exe`
iFolder 64-bit Client for Windows	Windows 7/ Windows 8	`ifolder3-windows-x64.exe`
iFolder Client for Intel Mac (Mono 2.4.2.3 is required)	Macintosh v10.4.11 and above	`ifolder3-mac.dmg`
Mono 2.4.2.3 Download for Mac	For more information on Mono, see Section 5.6, "Mono," on page 47	`MonoFramework-2.4.2.3_6.macos10.novell.x86.dmg`
XML Template for AutoAccount creation	Fore more information on AutoAccount creation, see Section 6.11, "Using a Response File to Automatically Create iFolder Accounts," on page 100	`AutoAccount.xml`
Passphrase Recovery Tool	Reset the passphrase and recover an encrypted iFolder	KeyRecovery.tar.gz

After expanding the install files, users are ready to install the iFolder client and its dependencies with the following files:

Table 6-3 *Install Files*

iFolder Client	Install Files
iFolder for Linux	ifolder3-3.9.2.xxxxx.0-1.1.i586.rpm simias-1.9.1.xxxxx.0-1.1.i586.rpm novell-ifolder-client-plugins-3.9.1.xxxxx.0-1.1.i586.rpm nautilus-ifolder3-3.9.1.xxxxx.1-1.1.i586.rpm ifolder3-3.9.2.xxxxx.0-1.1.x86_64.rpm simias-1.9.1.xxxxx.0-1.1.x86_64.rpm novell-ifolder-client-plugins-3.9.1.xxxxx.0-1.1.x86_64.rpm nautilus-ifolder3-3.9.1.xxxxx.1-1.1.x86_64.rpm
iFolder for Windows	`ifolder3-windows.exe`
iFolder for Windows (64 bits)	`ifolder3-windows-x64.exe`
iFolder for Macintosh	`ifolder3-mac.dmg`
Mono 2.4.2.3	`MonoFramework-2.4.2.3_6.macos10.novell.x86.dmg`

6.10.3 Installing the iFolder Client

For information about prerequisites and installation, see "Getting Started" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

6.11 Using a Response File to Automatically Create iFolder Accounts

Installing iFolder client and configuring an account on each desktop is a difficult task when the number of users is high. Without configuring an account, users cannot create iFolders or share iFolders on the system. For each user, you must provide a username and the server address with which they can configure an account using the iFolder Account Creation Wizard.To make these tasks simpler, it's useful to automate the process of installing and configuring iFolder. You can use a deployment manager such as Novell ZENworks to automate the process of iFolder installation.To make the iFolder account creation simpler and automatic, with little or no user interaction, you can use the Auto-account creation feature.

iFolder Auto-account creation facility provides you a user-friendly XML-based response file that helps you create accounts for multiple enterprise users. The response file contains the necessary information in XML format such as default credentials and server information to configure an account.You can use any deployment manager to distribute the client RPMs along with the customized response file to the user desktops.

- Section 6.11.1, "Response Files," on page 100
- Section 6.11.2, "Using a Response File to Deploy the iFolder Client," on page 103

6.11.1 Response Files

The response file is a user-specific XML file named `AutoAccount.xml` that contains the basic information to automatically create and configure an iFolder user account. A sample `AutoAccount.xml` is available for downloading in the Software Download page of the OES 2015 Welcome page. You can also use a script to generate a user-specific XML file with default credentials or with only the server information so that users can enter their credentials when the Account Creation Wizard is displayed. See "Sample Response File" on page 102 for more information. Use a deployment manager to push the response file to the following folders depending on the client platform.

Table 6-4 *Location of the Response file*

Platform	Location
Linux	`$HOME/.local/share/simias`
Windows XP	`%USERPROFILE%\Local Settings\Application Data\simias`
Windows 7 and Windows 8	`%LOCALAPPDATA%\simias`

IMPORTANT: The name of the response file `AutoAccount.xml` cannot be changed.

The mandatory fields in the response file are *Server* and *Username*. If you specify only the server name without giving the username, then all the inputs to the response file except the server name is ignored. If this is the case, the Account Creation Wizard is displayed with the server name pre populated with the value from the response file. The user should give the rest of the information in the iFolder Account Creation Wizard.

IMPORTANT: Regardless of whether a field is classified as mandatory or optional, the corresponding tags should always be present in the XML file for validation. The terms mandatory or optional apply only to the value of the tags and not to the tags themselves.

To get the status and details of the auto-account creation, see the `AutoAccount log` file. The path to the log file is specified in the log configuration file `UI.log4net`. The UI.log4net file allows you specify output location of the AutoAccount log files and what events are recorded at run time.The editable parameters of UI.log4net are similar to that of Simias.log4net. For more information, see Section 10.4, "Managing the Simias Log and Simias Access Log," on page 124.

Depending on the platform, the log configuration file is present in the following directory.

Table 6-5 *Location of the Configuration File*

Platform	Location
Linux	`$HOME/.local/share/simias`
Windows XP	`%USERPROFILE%\Local Settings\Application Data\simias`
Windows 7 and Windows 8	`%LOCALAPPDATA%\simias`

Response File Parameters

The following table gives the list of all parameters of the response file. All the parameters except Server and Username are optional. For optional fields, the default value is used when no explicit value is specified.

Table 6-6 *Response File Parameters*

Parameter	Possible Values	Default Value
default user account	True/false	True for the first account and false for the remaining accounts.
server	IP address	Mandatory field; no default value
user-id	Any string	Mandatory field; no default value
remember password	True/False	False
default-ifolder	True/False	True
path	Path string	**Linux:** *`HOME Directory/domain-name/user-id/Default`* **Windows:** `%APPDATA%\..\`*`domain-name\user-id`*
encrypted	True/False	False (If it is permitted by server)
securesync	True/False	False
force merge	True/False	False

Parameter	Possible Values	Default Value
prompt-to-accept-cert	True/False	False. This means that the certificate is accepted by default.
iFolder-creation-confirmation	True/False	True
iFolder-share-notify	True/False	True
conflict-notify	True/False	True
auto-sync enabled	True/False	True
auto-sync interval	Integer value	5

Sample Response File

Following is a typical example for the response file:

```
<?xml version="1.0" encoding="utf-8"?>

<auto-account xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="AutoAccount.xsd">

<user-account default="true">

        <server></server>

        <user-id></user-id>

        <remember-password>false</remember-password>

        <prompt-to-accept-cert>true</prompt-to-accept-cert>

        <default-ifolder default="true">

                <path></path>

                <encrypted>false</encrypted>

                <securesync>false</securesync>

                <forcemerge>false</forcemerge>

        </default-ifolder>

</user-account>

<general-preferences>

        <iFolder-creation-confirmation>true</iFolder-creation-confirmation>

        <iFolder-share-notify>true</iFolder-share-notify>

        <user-join-notify>true</user-join-notify>

        <conflict-notify>true</conflict-notify>

        <auto-sync interval="5">true</auto-sync>

</general-preferences>

</auto-account>
```

6.11.2 Using a Response File to Deploy the iFolder Client

NOTE: The procedure below shows one method of deployment. You can follow the method best suited to your needs.

1. Use the ZENworks deployment manager to distribute and install the iFolder client.
2. Depending on the platform used on the client machine that had the iFolder client auto-installed, push the `AutoAccount.xml` file to the path mentioned below:

   Table 6-7 *Platform-specific locations of Response file*

Platform	Location
Linux	`$HOME/.local/share/simias`
Windows XP	`%USERPROFILE%\Local Settings\Application Data\simias`
Windows 7 and Windows 8	`%LOCALAPPDATA%\simias`

   When the user starts the iFolder client for the first time, the account is created based on the information from the response file. If you have specified all the parameters for creating an account in the response file, then only password is requested from the user. Otherwise, the user must provide information for all the empty mandatory fields along with password when he or she logs in for the first time.

   The following sections describe the installation of iFolder using ZENworks on SLED and Windows.

Installation of iFolder on SLED using ZENworks Linux Management

Follow the steps given below to install and configure the iFolder client on SLED using ZENworks. Before you begin with the installation process, ensure the following:

- ZENworks Linux Management (ZLM) agent is installed and running on the machines where you want to install iFolder using ZENworks.
- Your system meets the iFolder requirements. For more information, see Chapter 5, “Prerequisites and Guidelines,” on page 45.

Create a bundle

1. Open the browser and login to ZLM Server web console.
2. Click the *Bundles* tab.
3. On the Bundles panel, select *New* > *Bundle* to launch the Create New Bundle Wizard.
4. In the Select Bundle type page, select the *File Bundle* option and click *Next*.
5. In the Name and Description page, enter a name, display name, location, and description for the bundle. Click *Next*.
6. In the Files page, add the files that you want to include in the bundle. To do this, do the following:
   1. Select *Add* > *Upload* to display the File Upload dialog box.
   2. Specify the destination where the file needs to be copied in the *Destination* field. For example, specify `/home` in the *Destination* field.

3. Specify the permissions in the *Permissions* field.
4. Select the target platform from the *Target Platforms* list.
5. Click the *Browse* button to browse to the location where `folder3-linux.tar.gz` is present and add the file.
6. Click the *OK* button.

NOTE: Ensure that the `Unpack` option in the Files page is not selected.

Similarly, add the `install-ifolder-script.sh` and `AutoAccount.xml` file to the bundle.

NOTE: While adding the file `AutoAccount.xml` to the bundle, you must specify the destination as `$HOME/.local/share/simias`.

---

7 After adding all the three files to the bundle, click *Next*.

8 In the Scriptable Actions page, click *New* to display the New Scriptable Action dialog box.

9 Select `Post-Installation` from the `Scriptable Action` list.

10 Select *Define your own script* from the *Script to run* list.

11 In the *Script content* field, add the following script:

```
cd /home
sh install-ifolder-script.sh
```

12 Click *OK* to close the New Scriptable Action dialog box and then click *Next*.

13 In the Summary page, you can view information about the bundle that you are creating and then click *Finish*.

Assign a Bundle

1 Click the `Bundles` tab on the ZLM Server web console.

2 On the Bundles panel, click the bundle created by you.

3 In the Assignments panel, click *Add* to launch the Assign Bundle Wizard.

4 In the Devices to be Assigned page, click *Add* to display the Select Devices dialog box.

5 Select the workstations that you want to assign the bundle to.

6 Confirm the selected workstations under the Selected list and click *OK* to close the dialog box. Click *Next*.

7 In the Bundle Options page, select the *Deploy and install immediately (when this wizard completes)* option and click *Next*.

8 Click *Finish*.

Installation of iFolder on Windows using ZENworks Configuration Management

Follow the steps given below to install and configure the iFolder client on Windows using ZENworks. Before you begin with the installation process, you must ensure that ZENworks agent is installed and running on the Windows machines where you want to install iFolder using ZENworks.

Create a Bundle

1. Open a browser and login to ZENworks Control Center
2. Click the *Bundles* tab.
3. On the Bundles panel, select *New* > *Bundle* to launch the Create New Bundle Wizard.
4. In the Select Bundle type page, select the *Windows Bundle* option and click *Next*.
5. Select *Empty Bundle* from the New Bundle Category and click *Next*.
6. In the Define Details page, fill in the following fields and click *Next*:

   Bundle Name: Specify a bundle name

   Folder: Specify the name or browse to the folder where you want the bundle to reside.

   Icon: Browse and specify the icon that you want to use for installation of a bundle. This is not a mandatory field.

   Description: Provide a brief description about the bundle. This is not a mandatory field.
7. Click *Finish*.

Specify the Windows Executable

1. After a bundle is created, click the bundle and then click the *Actions* tab.
2. In the Install tab, select *Add* > *Launch Windows Executable* to display the Add Action- Launch Windows Executable dialog box.
3. Specify the network path of the iFolder executable in the *Command* field.
4. Specify the command line parameters for a silent install in the *Command Line Parameters* field. The parameters for a silent install are:

   ```
   ifolder3-windows.exe /s /v"/qn INSTALLDIR=\"C:\Program Files\iFolder3\"
   ALLUSERS=1"
   ```

   Replace the location C:\Program Files\iFolder3 with the location you want to install iFolder.

   WARNING: The silent install command installs iFolder and reboots the workstations without any user intervention.

   ---
5. Click *OK* to close the Add Action- Launch Windows Executable dialog box.
6. Click *Apply*.

Add the AutoAccount.xml file to the Bundle

1. Click the bundle and then click the *Actions* tab.
2. In the Install tab, select *Add* > *Install File(s)* to display the Add Action- Install File(s) dialog box.
3. Click *Add* to display the Select Files dialog box.
4. Click *Add* to browse and specify the `AutoAccount.xml` file.
5. Specify `%USERPROFILE%\Local Settings\Application Data\simias` in the *Destination Directory* field.
6. Select the appropriate option from the *Copy Option* list.
7. Click *OK* to close the Add Action- Install File(s) dialog box.
8. Click *Apply*.

Increment the Bundle Version

1. Click the bundle that you have created.
2. In the *Summary* tab, click *Increment Version* to change the version number of the bundle.

Assign Bundle

1. Click the bundle and then click the *Relationships* tab.
2. In the Device Assignments panel, click *Add* to display the Select Objects dialog box.
3. Select the workstations that you want to assign the bundle to.
4. Confirm the selected workstations under the Selected list and click *OK* to close the dialog box.
5. Click *Next*.
6. In the Schedules page, select the *Distribution Schedule* option and click *Next*.
7. In the Bundle Distribution Schedule page, select *Now* from the *Schedule Type* list and click *Next*.
8. Click *Finish* to assign the bundle.

6.12 Updating Novell iFolder 3.9.x

As patches become available for iFolder, they are delivered to the OES Patch channel. Any iFolder server or client patches or updates can be installed through ZENworks Linux Management (formerly Red Carpet) channels.

- The iFolder client checks for updates on the server whenever a user logs in, and prompts the user to install a new update if it exists. The user must update the iFolder client, when prompted for version change. For more information about server and client compatibility, see Section E.4, “Server Client Support,” on page 229.
- Patches or updates to the iFolder client for Linux must be delivered through a customer-hosted channel, so that your users have access to them. For information on how to set up a customer-hosted channel, please see documentation for ZENworks Linux Management.

6.13 Updating Mono for the Server and Client

Novell iFolder server supports only mono-addon version 2.6.7 which is included in its install software. Any updates to this will be available from regular OES patch channel.

For iFolder clients, you can upgrade the Mono packages available in the SUSE distribution through Mono upgrade channel unless otherwise the iFolder Administrator guide specifies a particular version. For client, XSP RPMs must be at least 1.1.18 or later.

Please check our online documentation to see if we explicitly support that version and to learn any necessary steps to make the upgrade work correctly. For information, see the latest version of the online documentation on the Novell iFolder 3.9 Documentation Web site (http://www.novell.com/documentation/ifolder3).

6.14 Uninstalling iFolder Enterprise Server

Use YaST to uninstall the iFolder enterprise server `.rpm` file. Uninstalling iFolder software does not remove the Simias store, including the config files available in the `/etc/apache2/conf.d`.

When the server is re-installed, each of the iFolder clients must remove the old iFolder account and re-create it, even if the server IP address for the iFolder account has not changed. Users must also set up iFolders and share relationships again.

6.15 What's Next

You have now installed and configured your Novell iFolder enterprise server and provisioned iFolder services for users. To set up system policies for iFolder services, continue with Chapter 11, "Managing iFolder Services via Web Admin," on page 147.

Provisioned iFolder users can install the Novell iFolder client on their workstations, create iFolders, and share iFolders with other authorized Novell iFolder users. For information, see the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

7 Migrating iFolder Services

The OES 2015 Migration Tool has a plug-in architecture and is made up of Linux command line utilities with a GUI wrapper.

You can migrate Novell iFolder 3.2 and iFolder 2.*x* to Novell iFolder 3.9 or later versions. Migration can be done either through the GUI Migration Tool or through the command line utilities.

To get started with migration, see "Overview of the Migration Tools" in the *OES 2015: Migration Tool Administration Guide*.

For information on iFolder Migration, Upgrade and Coexistence see "Migrating iFolder to OES 2015" in the *OES 2015: Migration Tool Administration Guide*

8 Running Novell iFolder in a Virtualized Environment

Novell iFolder runs in a virtualized environment just as it does on a physical server and requires no special configuration or other changes.

To get started with virtualization, see Introduction to Xen Virtualization (http://www.novell.com/documentation/vmserver/virtualization_basics/data/b9km2i6.html) in the Getting Started with Virtualization Guide (http://www.novell.com/documentation/vmserver/virtualization_basics/data/front_html.html).

To get started with third-party virtualization platforms, such as Hyper-V from Microsoft and the different VMware product offerings, refer to the documentation for the product that you are using.

8.1 What's Next

To learn more about managing Novell iFolder, continue with Chapter 10, "Managing an iFolder Enterprise Server," on page 123.

9 Clustering iFolder Servers with Novell Cluster Services for Linux

This section discusses how to configure a Novell iFolder server cluster, using Novell Cluster Services (NCS) for Linux.

- Section 9.1, “Prerequisites for Clustering iFolder Services,” on page 113
- Section 9.2, “Installing Novell Cluster Services for Linux,” on page 113
- Section 9.3, “Configuring iFolder Servers on a NCS for Linux Cluster,” on page 114
- Section 9.4, “Updating Cluster Shared Pool Load and Unload Scripts,” on page 116
- Section 9.5, “Managing Cluster Resource for iFolder,” on page 116
- Section 9.6, “Sample Load Scripts for iFolder Clusters,” on page 116
- Section 9.7, “Sample Unload Scripts for iFolder Clusters,” on page 118
- Section 9.8, “Sample Monitor Scripts for iFolder Clusters,” on page 120

For information about Novell Cluster Services (NCS), see the *OES 2015: Novell Cluster Services for Linux Administration Guide*.

9.1 Prerequisites for Clustering iFolder Services

Each node in your iFolder cluster must satisfy the following requirements:

- “Prerequisites and Guidelines” on page 45.
- Prerequisites and requirements for Novell Cluster Services for Linux. For information, see “Installing, Configuring, and Repairing Novell Cluster Services” in the *OES 2015: Novell Cluster Services for Linux Administration Guide*.

9.2 Installing Novell Cluster Services for Linux

For each node in the planned cluster:

IMPORTANT: If you are using iSCSI for shared disk system access, ensure that you have configured iSCSI initiators and targets prior to installing Novell Cluster Services.

---

1. Make sure each node in the cluster satisfies the requirements in Section 9.1, “Prerequisites for Clustering iFolder Services,” on page 113.
2. Install and configure Novell Cluster Services (NCS) on the Open Enterprise Server (OES) servers you plan to use in iFolder cluster.

   For information on installing NCS, see the section “Installing, Configuring, and Repairing Novell Cluster Services” in the *OES 2015: Novell Cluster Services for Linux Administration Guide*.

3 Ensure that there is at least one shared storage setup that is cluster enabled, either Linux POSIX Volume(s) or NSS volume(s).

4 Continue with Section 9.3, “Configuring iFolder Servers on a NCS for Linux Cluster,” on page 114.

9.3 Configuring iFolder Servers on a NCS for Linux Cluster

The following procedure describes how to configure Novell iFolder services on Novell Cluster Services for Linux cluster. You can optionally add Web Access and Web Admin for iFolder to the cluster.

IMPORTANT: Do not create an iFolder Cluster Resource at this time; it is configured after you finish setting up iFolder services on the cluster.

---

1 For each node in the cluster, install iFolder services:

   1a In YaST, install iFolder server, Web Admin console, and Web Access console, but do not configure services at this time.

   For information, see Section 6.1, “Installing iFolder on an Existing OES Server,” on page 49.

   1b Repeat the install on each node in the cluster, then continue with Step 2 on page 114.

2 Ensure that the configured shared storage resource is online on the Master node, then configure the iFolder server by using the steps given below:

   2a Ensure that the shared resource is mounted on the Master node.

   For example:`/media/nss/NSSVOL`.

   Mounting will not be done, if the resource is on a different node. Migrate that resource to the Master node.

   2b In YaST, configure iFolder enterprise server.

   For information, see Section 6.2, “Deploying iFolder Server,” on page 51.

   For the System Store Path, specify the mount point of the shared volume that you created in Step 2a on page 114.

   IMPORTANT: You must ensure that you use pool IP or iFolder cluster resource IP while configuring iFolder services (Server, Web Access, Web Admin).

   At the end of the configuration, open your Web browser to the iFolder server to make sure it is running.

   `http://`*`192.168.1.1`*`/simias10/Simias.asmx`

   Replace *192.168.1.1* with the pool IP or iFolder cluster resource IP that you specified while configuring iFolder services. If everything is working properly, you should get an authentication prompt. On authentication, if you receive an error indicating that access to path is denied, follow the instructions outlined in Step 2c.

   2c If you are using an NSS volume to store user data, you must set up NSS file system trustee rights for the Web server user object wwwrun before restarting your web server.

   2c1 At a terminal console prompt, log in as the root user or equivalent, then enter

   ```
   rights -f /media/nss/NSSVOL/iFolder_Data -r rwfcem trustee
   wwwrun.ou.o.treename
   ```

/media/nss/NSSVOL: The `/media/nss/NSSVOL` is the cluster shared storage resource of the Master node.

iFolder_Data: It is the directory that is configured in Step 2b on page 114 to be used as the iFolder store location.

wwwrun.ou.o.treename: This is the FDN of the configured apache user that is LUM enabled to be used with the Apache Web Server.

NOTE: You must ensure that LUM is configured and running successfully.

2c2 Open your Web browser and enter `http://192.168.1.1/simias10/Simias.asmx` to make sure iFolder Server is running.

Replace 192.168.1.1 with the IP address of the cluster resource you have made online or migrated in Step 2a on page 114. If everything starts working properly, you get an authentication prompt.

2c3 Enter admin credentials and verify if you are able to log in to the page successfully. A successful login indicates that the iFolder server is configured properly. Then close the Web Browser.

2c4 To configure Web Access in YaST:

- For the Web Access Alias, specify an alias such as `/ifolder`. Use the same alias on all nodes when you configure them later.
- For the iFolder Server URL, specify the IP address or the DNS entry pointing to the cluster resource.

2c5 To configure Web Admin in YaST:

- For the Web Admin Alias, specify an alias such as `/admin`. Use the same alias on all nodes when you configure them later.
- For the iFolder Server URL, specify the IP address or the DNS entry pointing to the cluster resource.

2c6 Issue the following command:

```
/opt/novell/ifolder3/bin/ifolder_cluster_setup <Data Path>
```

For instance, if the Data Path is `/media/nss/NSSVOL/iFolder_Data, then issue the following command:`

```
/opt/novell/ifolder3/bin/ifolder_cluster_setup  /media/nss/NSSVOL/
iFolder_Data
```

3 Configure iFolder services on each of the remaining nodes in the cluster by doing the following:

NOTE: Before configuring iFolder service on the remaining node(s), you must migrate the cluster pool or iFolder cluster resource from the master node to the remaining node(s). However, you must ensure that before you migrate, you must stop the ifolder service. You can achieve this by executing the command:

```
/opt/novell/ifolder3/bin/ifolder_shutdown
```

3a Run the following command: `/opt/novell/ifolder3/bin/ifolder_cluster_setup <Data Path>`. On executing this command, you will be prompted to configure Web Admin and Web Access. You may then choose to configure Web Admin and Web Access on a node.

3b Start Apache on this node.

```
/etc/init.d/apache2 start
```

3c Repeat Step 3 on page 115 to configure any additional nodes in your iFolder cluster.

NOTE: Repeat Step 3 on page 115 after upgrade of every node from OES 2 SP3 or later versions to OES 2015 iFolder.

9.4 Updating Cluster Shared Pool Load and Unload Scripts

1. In iManager Roles and Tasks, click *Clusters* > *Cluster Manager*.
2. Select the cluster object that has the cluster pool containing the iFolder shared volume.
3. Edit the load script for the cluster pool and add the following line at the end of the load script:

   ```
   exit_on_error /opt/novell/ifolder3/bin/ifolder_start
   ```

   Similarly, edit the unload script for the cluster pool and add the following line at the beginning of the unload script:

   ```
   ignore_error /opt/novell/ifolder3/bin/ifolder_shutdown
   ```

For information on sample load and unload scripts, see Section 9.6, “Sample Load Scripts for iFolder Clusters,” on page 116 and Section 9.7, “Sample Unload Scripts for iFolder Clusters,” on page 118

9.5 Managing Cluster Resource for iFolder

In iManager Roles and Tasks, expand the *Clusters* role, then click *Cluster Manager* to manage the resource for iFolder and bring it online.

9.6 Sample Load Scripts for iFolder Clusters

You can obtain the sample load scripts using iManager. To do this, follow the steps given below:

1. In iManager Roles and Tasks, click *Clusters* > *Cluster Options*.
2. Click iFolder_template and then click the *Scripts* tab to display the sample load and unload scripts.

- Section 9.6.1, “Linux POSIX File System,” on page 116
- Section 9.6.2, “NSS File System,” on page 117

9.6.1 Linux POSIX File System

If your shared volume uses a Linux POSIX file system, use the following load script as a guide:

```
##### Linux Traditional File System Sample Load Script #####

#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

#define the IP address
RESOURCE_IP=10.10.189.136

#define the file system type
MOUNT_FS=ext3

#define the volume group name
VOLGROUP_NAME=ifoldervg
```

```
#define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/ifoldervol

#define the mount point

MOUNT_POINT=/mnt/ifolder

#activate the volume group
exit_on_error vgchange -a ey $VOLGROUP_NAME

#mount the file system
exit_on_error mount_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

#add the IP address
exit_on_error add_secondary_ipaddress $RESOURCE_IP

#start iFolder
exit_on_error /opt/novell/ifolder3/bin/ifolder_start

#return status

exit 0

##################################################
```

9.6.2 NSS File System

If your shared volume uses the NSS file system, use the following load script as a guide:

```
##### NSS File System Sample Load Script #########

#mount the file system

##MYPOOL is the name of your NSS pool

##MYVOL is the name of your NSS volume

#nss /poolactivate=MYPOOL

#exit_on_error nssmount -n MYVOL

#add the IP address

##xx.xx.xx.xx is your 'highly available' IP address

#exit_on_error add_secondary_ipaddress xx.xx.xx.xx

# start the service

exit_on_error /opt/novell/ifolder3/bin/ifolder_start

#return status

exit 0

##################################################
```

9.7 Sample Unload Scripts for iFolder Clusters

You can obtain the sample unload scripts using iManager. To do this, follow the steps given below:

1. In iManager Roles and Tasks, click *Clusters* > *Cluster Options*.
2. Click iFolder_template and then click the *Scripts* tab to display the sample load and unload scripts.

- Section 9.7.1, “Linux POSIX File System,” on page 118
- Section 9.7.2, “NSS File System,” on page 118
- Section 9.7.3, “Troubleshooting,” on page 119

9.7.1 Linux POSIX File System

If your shared volume uses a Linux POSIX file system, use the following unload script as a guide:

```
##### Linux Traditional File System Sample Unload Script #####

#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

#define the IP address
RESOURCE_IP=10.10.189.136

#define the file system type
MOUNT_FS=ext3

#define the volume group name
VOLGROUP_NAME=ifoldervg

#define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/ifoldervol

#define the mount point
MOUNT_POINT=/mnt/ifolder

#stop iFolder
ignore_error /opt/novell/ifolder3/bin/ifolder_shutdown

#del the IP address
ignore_error del_secondary_ipaddress $RESOURCE_IP

#umount the volume
sleep 10 # if not using SMS for backup, please comment out this line

exit_on_error umount_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

#deactivate the volume group
exit_on_error vgchange -a n $VOLGROUP_NAME

#return status
exit 0

##################################################
```

9.7.2 NSS File System

If your shared volume uses the NSS file system, use the following unload script as a guide:

```
##### NSS File System Sample Unload Script ####################

#stop iFolder

ignore_error /opt/novell/ifolder3/bin/ifolder_shutdown

#del the IP address

##xx.xx.xx.xx is your 'highly available' IP address

#ignore_error del_secondary_ipaddress xx.xx.xx.xx

#umount the file system

##MYPOOL is the name of your NSS pool

##MYVOL is the name of your NSS volume

#umount /media/nss/MYVOL

#nss /pooldeactivate=MYVOL

#return status

exit 0

##################################################
```

NOTE: When OES 2 SP1 cluster setup is upgraded to OES 2 SP3, the load and unload scripts are not updated automatically. Post upgrade, the load and unload scripts must be updated with content from latest template file. For more information on script update, refer to *OES 2015: Novell Cluster Services for Linux Administration Guide*.

9.7.3 Troubleshooting

Linux does not allow you to umount a volume if any file is currently open. If your system is going comatose when you try to unload the cluster, it is probably because you have open user connections and files on the volume. You need to allow enough time for the connections to be closed before the umount is executed.

Add the following lines between the request to stop service and deleting the IP address:

```
#stop service otherwise

sleep 10

ignore_error fuser -k /$MOUNT-POINT

sleep 5
```

Replace `/$MOUNT-POINT` with the actual path of the mount point of your iFolder data store. For example, if the mount point is `/var/opt/novell/ifolder3/data`, add:

```
#stop service otherwise

sleep 10

ignore_error fuser -k /var/opt/novell/ifolder3/data

sleep 5
```

Tune the script until the cluster no longer goes comatose under an operational load when the unload script is called. If the system goes comatose under a full load, increase the sleep time until the cluster is able to successfully execute the unload instead of going comatose.

9.8 Sample Monitor Scripts for iFolder Clusters

- Section 9.8.1, “Linux POSIX File System,” on page 120
- Section 9.8.2, “NSS File System,” on page 120

9.8.1 Linux POSIX File System

If your shared volume uses a Linux POSIX file system, use the following monitor script as a guide:

```
#!/bin/bash

. /opt/novell/ncs/lib/ncsfuncs

function check_ifolder {

result=`ps -f -U wwwrun | awk '/mod_mono_server_(admin|ifolder|simias10)/
{i++;}END{print i}'`;

if [[ $result -ne '3' ]];then return 1; else return 0; fi;

}

# define the IP address

RESOURCE_IP=a.b.c.d

# define the file system type

MOUNT_FS=reiserfs

#define the container name

container_name=name

# define the device

MOUNT_DEV=/dev/evms/$container_name/ifolder

# define the mount point

MOUNT_POINT=/mnt/ifolder

# check the file system

exit_on_error status_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

# check the IP address

exit_on_error status_secondary_ipaddress $RESOURCE_IP

# check iFolder

exit_on_error check_ifolder

# return status

exit 0
```

9.8.2 NSS File System

If your shared volume uses the NSS file system, use the following monitor script as a guide:

```
# define the IP address

RESOURCE_IP=a.b.c.d
```

```
#check the file system
##MYPOOL is the name of your NSS pool
exit_on_error status_fs /dev/evms/MYPOOL /opt/novell/nss/mnt/.pools/MYPOOL nsspool
##MYVOL is the name of your NSS volume
exit_on_error ncpcon volume MYVOL
# check the IP address
exit_on_error status_secondary_ipaddress $RESOURCE_IP
# check iFolder
exit_on_error check_ifolder
#return status
exit 0
```

10 Managing an iFolder Enterprise Server

This section describes how to manage your Novell iFolder enterprise server.

- Section 10.1, “Starting iFolder Services,” on page 123
- Section 10.2, “Stopping iFolder Services,” on page 123
- Section 10.3, “Restarting iFolder Services,” on page 123
- Section 10.4, “Managing the Simias Log and Simias Access Log,” on page 124
- Section 10.5, “Backing Up the iFolder Server,” on page 125
- Section 10.6, “Recovering from a Catastrophic Loss of the iFolder Server,” on page 126
- Section 10.7, “Using TSAIF to Back Up and Restore the iFolder Store,” on page 127
- Section 10.8, “Recovering iFolder Data from File System Backup,” on page 133
- Section 10.9, “Moving iFolder Data from One iFolder Server to Another,” on page 134
- Section 10.10, “iFolder Data Recovery Tool,” on page 135
- Section 10.11, “Changing The IP Address For iFolder Services,” on page 142
- Section 10.12, “Securing Enterprise Server Communications,” on page 143

10.1 Starting iFolder Services

iFolder services start whenever you reboot the system or whenever you start Apache services.

As a root user, enter the following command at the terminal console:

```
/etc/init.d/apache2 start
```

10.2 Stopping iFolder Services

iFolder services stop whenever you stop the system or whenever you stop Apache services.

As a root user, enter the following command at the terminal console:

```
/etc/init.d/apache2 stop
```

10.3 Restarting iFolder Services

If you need to restart iFolder services, you must stop and start Apache services:

As a root user, enter the following command at the terminal console:

```
/etc/init.d/apache2 stop
/etc/init.d/apache2 start
```

Avoid using the Apache Restart command, instead you must use Apache reload command. If any other modules using the Apache instance do not exit immediately in response to the Apache Restart command, iFolder might hang.

10.4 Managing the Simias Log and Simias Access Log

On the iFolder enterprise, there are two logs that track events:

- **Simias Log:** The `/simias/log/Simias.log` file contains status messages about the health of the Simias Service.
- **Simias Access Log:** The `simias/log/Simias.access.log` file contains file access events for data and metadata about iFolders, users, membership in shared iFolders, and so on. It reports the success of the event and identifies who did what and when they did it. For example, if a file was deleted on the server, it identifies the user who initiated the deletion.

Review the logs whenever you need to troubleshoot problems with your iFolder system.

The Simias Log4net file (`/simias/Simias.log4net`) allows you specify output location of the log files and what events are recorded at run time. Its parameters are based on, but not compliant with, the Apache Logging Services (http://logging.apache.org/log4net). The following parameters are modifiable:

Parameters	Description	Examples

Location and name of the log
 	
`<file value="`*pathname*`" />`
	The location of the log file. Specify the full path where the file is located on the computer, including the volume, intermediate directories, and filename.	`<file value="<iFolder Data>/simias/log/Simias.log">`
		
		`<file value="<iFolder Data>/simias/log/Simias.access.log" />`

Maximum size of the log file `<maximumFileSize value="`*size*`" />`	The maximum size of the log file. When the file grows to this size, the content is rolled over into a backup file and the recording continues in the now-empty file. A period and sequential number are appended to the filename of the backup log files, such as `Simias.log.1` and `Simias.log.2`. For *size*, specify the number and unit, such as `10MB` or `20MB`, with no space between them.	`<maximumFileSize value="10MB" />`
How much logged data to retain `<maxSizeRollBackups value="`*number*`" />`	The maximum number of backup log files that are kept before they are overwritten. The log rolls over sequentially until the maximum number of backups are created, then overwrites the oldest log file.	`<maxSizeRollBackups value="10" />`

Parameters	Description	Examples

Level of Simias Services messages
 	
`<level value="status" />`
 	
(Use only for the `Simias.log`.)
	The type of messages or level of detail you want to capture for the log. Valid levels include the following:
	
	`OFF`
	`FATAL`
	`ERROR`
	`WARN`
	`INFO`
	`DEBUG`
	`ALL`
		`<level value="ERROR" />`

Fields to report for file access events
 	
`<header value="layout" />`
 	
(Use only for the `Simias.access.log`.)
	Specify which fields to report and the order you want them to appear for each entry. Valid fields include the following:
	
	`date`
	`time`
	`method` (program call or event)
	`status` (success or failure)
	`user`
	`uri` (relative path of the file in an iFolder)
	`id` (node key)
	
	The fields are pattern delimited (`**`) by default. Use this pattern to add additional fields.
		`<header value="#version: 1.0

#Fields:**date**time**method**status**user**uri**id**
" />`

In the Log4net terminology, each output destination is defined in an XML `appender` tag. If you do not want to log events for the Simias Service or for file access, comment out (`!--`) the related `appender` tag and its child elements for that log file.

10.5 Backing Up the iFolder Server

1. Find and note down the Simias Data Store(s)

   You can find the default location of the Simias store directory under Data Store section in the Server Details page of the Web Admin console and additional data stores if configured. For more information on this, see Step 8 on page 164 and "Enable or Disable Data Store:" on page 165.

2. Open a terminal console, login as root or root equivalent user, and enter the following command to stop the iFolder server.

   ```
   /etc/init.d/apache2 stop
   ```

3. Stop the iFolder mono process if running.

   ```
   pkill mono
   ```

4. Use your normal file system backup procedures to back up all the Data Stores.

5 Start the iFolder server by entering the following command as root user:

```
/etc/init.d/apache2 start
```

10.6 Recovering from a Catastrophic Loss of the iFolder Server

If the iFolder server configuration or data store becomes corrupted, use your iFolder backup files to restore the database to its last good backup. Restoring the iFolder server to the state it was in at the time of the backup also reverts the iFolders on any connected iFolder clients to that same state.

IMPORTANT: All changes made since the time of the backup will be lost on all connected clients.

Consider the following implications of restoring iFolder data:

- Any new file or directory is deleted if it was added to an iFolder since the time of the backup.
- Any file that was modified is reverted to its state at the time of the backup.
- Any file or directory is restored if it was deleted since the time of the backup.

Before restoring the iFolder server, consider notifying all users to save copies of any files or directories they might have modified in their iFolders since the time of the last backup. After the iFolder server is restored, they can copy these files or directories back into their respective iFolders

1 Notify users to save copies of iFolders or files that have changed since the time of the backup you plan to use for the restore.

2 Stop the iFolder server by entering the following command as root user:

```
/etc/init.d/apache2 stop
```

3 Remove the following corrupted data:

- Simias store directories

  The default location is `/var/simias/data/simias`.

  If there are multiple store, ensure that the corresponding data is also removed.

4 Use your normal iFolder system restore procedures to restore the following data to its original locations:

- Simias store directories

  The default location is `/var/simias/data/simias`.

  Restore the additional Simias store directories to their respective locations, if multiple store paths has been configured.

  IMPORTANT: Be careful not to modify anything else under the Simias store directory.

  ---

5 Start the iFolder server by entering the following command as root user:

```
/etc/init.d/apache2 start
```

6 Notify users that they can return their saved files to their iFolders for upload to the server. Users should coordinate this with other shared members of the iFolder to avoid competing updates.

10.7 Using TSAIF to Back Up and Restore the iFolder Store

The Target Service Agent (TSA) for Novell iFolder supports the back up of the iFolder store.

- Section 10.7.1, “Understanding TSAIF,” on page 127
- Section 10.7.2, “Syntax,” on page 128
- Section 10.7.3, “iFolder Path Options,” on page 128
- Section 10.7.4, “iFolder Path Examples,” on page 129
- Section 10.7.5, “SMSConfig Options,” on page 130
- Section 10.7.6, “TSAIF and SMSConfig Examples,” on page 131
- Section 10.7.7, “NBackup Options,” on page 131
- Section 10.7.8, “TSAIF and NBackup Examples,” on page 132
- Section 10.7.9, “Additional Information,” on page 133

10.7.1 Understanding TSAIF

iFolder TSA

Novell Storage Management Services (SMS) is an API framework that backup applications consume to provide a complete backup solution. The SMS framework is implemented by two main components: The Storage Management Data Requester and the Target Service Agent.

The TSA provides an abstraction of a particular backup target. The TSA uses native interfaces to read target data and transforms it to a continuous stream of data objects. The data objects are formatted in the ECMA standard System Independent Data Format (SIDF).

The TSA for iFolder (TSAIF) provides an implementation of the SMS API for an iFolder store. Backup applications, such as nbackup(1), can make use of its features by writing to the SMS API.

iFolder and Simias

iFolder is built upon Simias technology. Simias is a general-purpose object repository that provides a foundation for building collaborative solutions. A Simias Collection store contains Collection objects. At a minimum, a Simias Collection store contains a Local Database Collection and one or more Domain Collections. The Local Database Collection controls access to the physical storage of the Collection store on the file system. A Domain Collection contains a list of members in a given domain. For example, a Domain might contain all the members from a given LDAP directory. Each Collection is owned by exactly one Domain member.

An iFolder is a type of Simias Collection that has a root directory on the file system. Each file or subdirectory in the iFolder’s root directory has a corresponding FileNode or DirNode in the Collection. An iFolder store is a Simias Collection store that contains one or more iFolders and includes the directories and files associated with the iFolders.

For more information on the iFolder and Simias technologies, see the iFolder Project at www.ifolder.com (http://www.ifolder.com).

iFolder TSA Granularity

TSAIF supports creating archives that contain the following:

- The entire iFolder store
- All iFolders owned by a specified Domain member
- An individual iFolder

TSAIF supports restoring the following:

- The entire iFolder store
- All iFolders owned by a specified Domain member
- An individual iFolder
- An individual subdirectory in an iFolder
- An individual file in an iFolder

The entire iFolder store should be backed up regularly. In certain cases, a backup administrator might choose to back up an individual iFolder or to back up all iFolders owned by a specific owner. These special-case archives can be restored only to the same iFolder store from which they were backed up.

IMPORTANT: If you are restoring an entire iFolder and want to ensure that it is in the exact state it was in when it was backed up, you should first delete it from the server using a client or the iFolder Web Admin console or Web Access console.

Deleting the iFolder is not necessary to restore any or all of the files in the iFolder; the difference is in what metadata is given preference during the restore. If you do not delete the iFolder before restoring, the attributes of the iFolder, such as the owner, members, file type or size restrictions, remain as they are in the current version.

10.7.2 Syntax

At an OES server terminal console, enter

```
smsconfig -l tsaif [OPTION]...
```

The `-l` option registers the TSAIF with the Storage Management Data Requester (SMDR).

TSAIF uses the `libtsaif.so` file. The library implements all the necessary service functions to backup an iFolder target.

10.7.3 iFolder Path Options

The top-level resource for an iFolder store is `/` (a single forward slash) and represents the root of the iFolder store. The paths for iFolder data objects are specified relative to the root of the iFolder store, using the syntax of the Network File System (NFS) namespace. iFolder paths are logical paths into an iFolder store and do not correspond directly to file system paths.

Parameter	Description

`path`	iFolder path such as the following:
	`/`
	`/owner`
	`/owner/collection`
	`/owner/collection/relative-path`

`owner`	`owner-name.owner-id`
`owner-name`	Collection owner name (`Simias.Storage.Collection.Owner.Name`)
`owner-id`	Collection owner ID (`Simias.Storage.Collection.Owner.ID`)
`collection`	`collection-name.collection-id`
`collection-name`	Collection name (`Simias.Storage.Collection.Name`)
`collection-id`	Collection ID (`Simias.Storage.Collection.ID`)

`relative-path`	Relative path such as
	`file`
	`subdir`
	`subdir/relative-path`

`file`	name of file on file system
`subdir`	name of subdirectory on file system

The `\fIowner-id\fR` and `\fIcollection-id\fR` are required because `\fIowner-name\fR` and `\fIcollection-name\fR` are not guaranteed to be unique. Using both the name and ID properties to identify Collections and Collection owners provides a “friendly” name along with the required unique identifier.

In many configurations, the names of Collections and Collection owners are unique. For example, if Domain members are obtained from an LDAP directory, it is not likely that two members would have the same username. Likewise, it would be unusual for an owner to give two iFolders the same name.

Although a backup application must pass both the name and ID to TSAIF, it might display only the name to the backup administrator to simplify the user interface. The ID would need to be displayed to the backup administrator only when two Collections, or two Collection owners, have the same name and the backup administrator wants to perform an operation on only one of them.

The name of the Collection or Collection owner can be obtained by stripping off the pattern

```
".????????-????-????-????-???????????"
```

from the first two components of the path TSAIF returns to the backup application.

10.7.4 iFolder Path Examples

The following examples show how to use iFolder paths to backup and restore data at different levels in the iFolder store.

`/`

Back up or restore the entire iFolder store.

```
/myOwner.12345678-1234-1234-1234-123456789abc
```

Back up or restore all Collections owned by `myOwner`.

```
/myOwner.12345678-1234-1234-1234-123456789abc/myCollection.22345678-1234-1234-
1234-123456789abc
```

Back up or restore the Collection named `myCollection`. If the Collection is an iFolder, all files and directories in the iFolder will be backed up or restored along with the Simias data in the Collection store.

To backup and restore individual or group of files or subdirectories, use the backup engine- supported file filters. These file filters perform the include or exclude operations for selective backup and restore.

10.7.5 SMSConfig Options

The TSAIF command is not a standalone shell command; it is exercised using smsconfig. All configuration options are managed via smsconfig. The TSAIF can be configured during registration and the configuration persists until TSAIF is unloaded.

All long options (options that have the format `--optionname`) are case insensitive.

Option	Command
`--help`	Displays the options supported by the TSA.
`--ReadBufferSize`	This is the amount of data (Bytes) read from the Simias store and/or file system by a single read operation. This switch is based on the buffer sizes used by the applications. For example, if the application requests 32 KB of data for each read operation, set the buffer size to 32 KB to allow the TSA to service the application better. This value works well with Simias store and/or file system reads if set in multiples of 512 Bytes. The default value is 64 KB.
`--ReadThreadsPerJob`	This enables the TSA to read data ahead of the application request during backup. This switch is based on the number of processors in the system. This switch can also be used to influence the disk activity based on system configuration. The default value is 4.
`--ReadThreadAllocation`	This sets the maximum number of read threads that process a data set at a given time. This determines the percentage of ReadThreadsPerJob that should be allocated to a data set before proceeding to cache another data set. This enables the TSA to store a cache of data sets in a non sequential manner. This sets all read threads to completely process a data set before proceeding to another data set. The default value is 100.
`--ReadAheadThrottle`	This sets the maximum number of data sets that the TSA caches simultaneously. This prevents the TSA from caching parts of data sets and enables complete caching of data sets instead. Use this switch along with the ReadThreadAllocation switch. The default value is 2.
`--CacheMemoryThreshold`	This is used to specify the percentage of available server memory that the TSA can utilize to store cached data sets. This represents a maximum percentage value of available server memory that the TSA uses to store cached data sets. The default value is 10% of the total server memory.

10.7.6 TSAIF and SMSConfig Examples

The following examples show how to perform typical TSAIF configuration for SMS.

```
smsconfig -l tsaif --help
```

Displays the options supported by the TSAIF.

```
smsconfig -l tsaif --readthreadsperjob=8
```

Sets the number of read threads that the TSAIF starts per job to 8.

```
smsconfig -l tsaif --readbuffersize=32768 --cachememorythreshold=15
```

Sets the read buffer size to 32KB and the maximum amount of cache memory that the TSAIF should use to 15%.

10.7.7 NBackup Options

TSAIF supports the following typical `nbackup(1)` options:

Option	Command
`--exclude-file=pattern`	Excludes all files matching the name (owner, folder, or file) or pattern for back up or restore. Use this option multiple times to exclude more than one pattern.
`-F, --full-paths`	Stores the full paths for both directories and files in the created archive.
`-k, --keep-old-files`	Does not overwrite existing files while extracting files from the archive. Files are overwritten if this option is not present.
`-N, --after-date=date`	Backs up files newer than date.
`-P, --password=password`	The password to connect to the TSA. The password can be supplied at runtime.
`-R, --remote-target=hostname`	Connects to the file system TSA of the host specified in hostname for backup. Use with the `--target-type` option.
`--target-type=target_name`	Connects to the TSA specified by `target_name`, where the target name is Linux, or iFolder.
`-T, --input-file=file`	Takes file containing fully qualified paths as input for creating archive. This file should contain one path per line.
`-U, --user=username`	Username to use while connecting to the TSA.

TSAIF does not support the following nbackup(1) options:

Option	Command
`-m, --move-to=path`	Extracts the archive to the given path. This does not work with TSAIF because iFolder puts files in a `SimiasFiles` directory.
`-r, --restore-to="backup_path new_path"`	Restores by replacing `backup_path` with `new_path`. This does not work with TSAIF because iFolder puts files in a `SimiasFiles` directory.

If TSAIF cannot back up or restore a file, it skips the file and returns a warning. This can occur for various reasons. When this occurs, `nbackup(1)` creates a file with a `.warn` extension that contains a list of each file that was skipped along with the date and time it was skipped and the error code that was returned.

If files are skipped, try to resolve the issue, then run the operation again.

If you are unable to identify why the file was skipped, try running the operation again when the server is less busy.

If files are skipped during a restore, and if relatively few files are skipped, try individually restoring each skipped file.

The back-up administrator should use root or root-equivalent system user for both back-up and restore.

10.7.8 TSAIF and NBackup Examples

The following examples show how to perform typical TSAIF backup and restore operations using NBackup.

Backup or Restore Task	Command
Full backup	`nbackup -cvf full.sidf -U root -P password --target-type=ifolder /`
Full restore	`nbackup -xvf full.sidf -U root -P password --target-type=ifolder`
Owner backup	`nbackup -cvf owner.sidf -U root -P password --target-type=ifolder /owner.id`
Owner restore	`nbackup -xvf owner.sidf -U root -P password --target-type=ifolder`
Owner restore from the full backup file `full.sidf`	`nbackup -xvf full.sidf -U root -P password --target-type=ifolder --extract-dir=/owner`
iFolder backup	`nbackup -cvf ifolder.sidf -U root -P password --target-type=ifolder /owner/collection.id`

Backup or Restore Task	Command

iFolder restore	`nbackup -xvf ifolder.sidf -U root -P password --target-type=ifolder`
	
	`nbackup -xvf owner.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection`
	
	`nbackup -xvf full.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection`
	
	If you are restoring an entire iFolder and want to ensure that it is in the exact state it was in when it was backed up, you should first delete the current iFolder from the server using a client or the iFolder 3 plug-in for iManager.
	
	Deleting the iFolder is not necessary to restore any or all of the files in the iFolder; the difference is in what metadata is given preference during the restore. If you do not delete the iFolder before restoring, the attributes of the iFolder, such as the owner, members, file type or size restrictions, remain as they are in the current version.

Subdirectory restore	`nbackup -xvf ifolder.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection/relative-path`
	
	`nbackup -xvf owner.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection/relative-path`
	
	`nbackup -xvf full.sidf -U root -P`

10.7.9 Additional Information

For more information about backup, see the following man pages on your iFolder enterprise server: `nbackup(1)`, `sms(7)`, `smdrd(8)`, `smsconfig(1)`, `tsaif.conf(5)`.

10.8 Recovering iFolder Data from File System Backup

You can recover the individual files and directories within an iFolder irrespective of its type. Use the normal file system restore procedure to restore them from a file system backup.

10.8.1 Recovering a Regular iFolder

1. Collect information that uniquely identifies the file or directory to be recovered, such as a combination of the following:
   - iFolder name, such as `MyiFolder`
   - iFolder owner
   - iFolder member list
   - Relative path of the file or directory, such as `/MyDir1/MyDir2/myfile.txt`
   - Time stamp or approximate time of the version desired
   - Other files or directories in the iFolder
2. On the iFolder server, use your normal file system restore procedures to restore the iFolder directory from backup to a temporary location.

For example, restore `/var/opt/novell/ifolder3/simias/SimiasFiles/62ba1844-6987-47fc-83ab-84bbd5d6130b/MyiFolder/MyDir1/MyDir2/MyFile` to `/tmp/MyFile`.

IMPORTANT: Do not restore the file to its original location, or to any location under the Simias store directory.

---

3 Compress and send the entire folder (`MyiFolder`) to the user via e-mail or other data transfer channel to restore the recovered file to the target iFolder.

Use one of the following methods:

- **Via E-Mail:** Send the restored files or directory to the iFolder owner or to any member who has the Write right to the iFolder.

  For example, e-mail the recovered file, such as `/tmp/MyFile`, to the user. A user with the Write right can restore the file to an iFolder simply by copying it back to the appropriate location on an iFolder client. For example, copy `MyFile` to `/home/`*`username`*`/MyiFolder/MyDir1/MyDir2/MyFile`.

- **Via Web Access:** In the Web Admin console, select the *iFolder* tab, search for the iFolder you want to manage, then click the link for the iFolder. On the iFolder page, click *Members*, then add yourself as a member of the target iFolder.

  In a Web browser, log in to iFolder Web Access console, browse to locate and open the iFolder, then navigate to the directory where the files were originally located. Upload the file to the iFolder. For example, upload `MyFile` to `MyiFolder/MyDir1/MyDir2/MyFile`. If necessary, create the directory you want to restore, then upload the files in it.

10.9 Moving iFolder Data from One iFolder Server to Another

You can relocate iFolder services and the iFolder data in the Simias Store from one iFolder server to another, such as if you want to migrate to a more powerful system.

NOTE: This procedure is not applicable for the iFolder 2.*x* servers.

---

1 Notify users that the iFolder server is going down.

2 Stop iFolder services. As a root user, enter the following command at the terminal console:

```
/etc/init.d/apache2 stop
```

3 Use your normal file system backup procedures to back up the following data:

- Simias store directory

  The default location is `/var/simias/data/simias`.

- Apache config files for iFolder

  The default location is `/etc/apache2/conf.d` and contain the following files:

  - `simias.conf`
  - `ifolder_admin.conf` (if available)
  - `ifolder_web.conf` (if available)

4 Install and configure iFolder on the target server, using the same configuration information and location as on the old computer, including the IP address.

5 In a terminal console on the target server, run `ifolder-admin-setup` and `ifolder-web-setup` to generate public keys in the server.

6 On the target server, use your normal file system restore procedures to restore the following data to its original locations:

- Simias store directory

  The default location is `/var/simias/data/simias`.

7 On the target server, copy the apache config files for iFolder to `/etc/apache2/conf.d` if it is not already available.

8 Start iFolder services. As a root user, enter the following command at the terminal console:

```
/etc/init.d/apache2 start
```

9 Notify users that the server is back up.

10 Disconnect the original server from the network, then uninstall iFolder to remove iFolder software and the iFolder data. Make sure to reconfigure its IP address before using it on the network again.

NOTE: You must ensure that the datapath (simias store directory) on source server and destination server is the same and iFolder server datapath is not changed while moving the iFolder data.

10.10 iFolder Data Recovery Tool

You use the iFolder Data Recovery tool to restore a user's backed-up data.

- Section 10.10.1, "Understanding the iFolder Data Recovery Tool," on page 135
- Section 10.10.2, "Prerequisites and Guidelines," on page 136
- Section 10.10.3, "Using the Data Recovery Tool," on page 136

10.10.1 Understanding the iFolder Data Recovery Tool

The iFolder Data Recovery tool is a command line utility that enables you to restore backed-up files, folders, or iFolders for any user. If an administrator has performed regular or incremental file system backups of all iFolder system data on the server, the data can be restored with this tool. iFolder data can be restored in its entirety or even at a granular level like a particular file or a folder. This tool also enables you to restore encrypted iFolders.

The tool provides the following functionality:

- Restoration of iFolders, folders, and files
- Two methods of data restoration:
  - **Local restore:** This method employs a direct copy of data from a temporary location (where the backup is restored) to the desired location, and makes the data available to the end user. This method of restoring data is faster than the Web-based method, because it uses a direct copy. It is also the only method you can use to restore a file that is larger than 1 GB. However, this method cannot be used to restore data to a remote iFolder server.
  - **Web-based restore:** This method uses HTTP to transfer the data and metadata from a temporary location to the desired location. This makes it possible to restore data to a remote iFolder server, but it is slower because it uses HTTP to send both data and metadata.

- Built-in intelligence to identify method to restore data based on whether the destination is on the same machine or a different one.
- It does not decrypt the contents of an encrypted iFolder in the process of restoring an encrypted iFolder.

10.10.2 Prerequisites and Guidelines

To successfully use the data recovery tool, use the following guidelines:

- You must ensure that iFolder service is stopped while taking file system backups.
- The administrator who runs the data recovery tool must have root or equivalent privileges.
- The data that needs to be restored must be backed up properly. Any corruption in the backed-up data stops the restore operation.
- To use the tool, you must first restore the backed-up data to a temporary location and then you must run the tool from the same place. You must ensure that the restored content retains the same rights or permissions that was assigned when it was backed up and you must ensure that the user wwwrun has access rights on the temporary location.
- To perform a restore operation, you need to know the location of the following data:
  - From the iFolder server data path, you need to know the location of the FlaimSimias files and directories. For instance, `FlaimSimias.01`, `FlaimSimias.lck`, `FlaimSimias.db`, and `FlaimSimias.rfl`.
  - `Simias.config`.
  - `Simias.log4net`.
  - `modules` directory.
  - Folder data (the actual file, folder, or iFolder data to be restored)
- If the data recovery tool quits with an error during the restore process, re-run the tool and use the `retry` option to complete the restore process.
- To restore a file that is larger than 1 GB in size, you must use the local restore method.
- Files are restored from iFolder and its immediate subfolder. The subsequent subfolders cannot be restored.

10.10.3 Using the Data Recovery Tool

The data recovery tool is available in `/opt/novell/ifolder3/bin`. It uses the following syntax:

```
ifolder-data-recovery <Operation> <Options>
```

Any path specified using the tool is the absolute path, unless the path is specified by using the relativepath option.

If there is a space in the path or filename, the path or filename must be specified within double quotes.

Usage

Operation	Description
--list	Lists iFolders owned by the specified user, and gives details such as name, iFolderid, and path (at the time of backup)

Operation	Description
--restore	Restores the requested data (File/Folder/iFolder) from the specified backup store or location
--retry	Resumes the restore operation that failed in the last run
--help	Displays help for the operation, options, and usage

Options	Description
--path=	The path of the `simias` files in the backup store. The `simias` files must be present in a directory named `simias`. The path must be the absolute path to the `simias` directory.
--backup-admin=	The login name of the administrator who performed the backup
--backup-password=	The password of the Administrator who performed the backup
--current-admin=	The administrator login name for current server
--current-password=	The password of the current server's Administrator
--server-url=	The URL of the server where data is to be restored
--user=	The username or ID of the user for whom the specified operation is to be performed
--ifolder-id=	The ID of the iFolder for which the specified operation is to be performed
--ifolder-path=	The absolute path (excluding the iFolder name) of the actual data to be restored
--relative-path=	The relative path of file or folder to be restored, starting from iFolder name
--restore-policies	Overwrites current iFolder policies with the policies of the iFolder from backup
--usewebaccess	The mode to use. Does not take any value.

Examples

To display help: `ifolder-data-recovery --help`

To list iFolders for a specified user: `ifolder-data-recovery --list --path <path of simias file in backup store> --backup-admin <admin login name for backup> --backup-password <password of the backup admin> --user=<username or ID of the user>`

To restore an iFolder: `ifolder-data-recovery --restore --path <path of simias file in backup store> --backup-admin <admin login name for backup> --backup-password <password of the backup admin> --current-admin <admin login name for current server> --current-password <password of the current server's admin> --server-url=<current ifolder server url> --ifolder-id=<ID of the iFolder for which restore operation is performed> --ifolder-path=<Parent level path for actual data to be restored>`

To restore a file or a folder: `ifolder-data-recovery --restore --path <path of simias file in backup store> --backup-admin <admin login name for backup> --backup-password <password of the backup admin> --current-admin <admin login name for current server> --current-password <password of the current server's admin> --server-url=<current ifolder server url> --ifolder-id=<ID of the iFolder for which restore operation is performed> --ifolder-path=<Parent level path for actual data to be restored> --relative-path=<Relative path of file or folder to be restored>`

To retry restore operation: `ifolder-data-recovery --retry --path <path of simias file in backup store> --backup-admin <admin login name for backup> --backup-password <password of the backup admin> --current-admin <admin login name for current server> --current-password <password of the current server's admin> --server-url=<current ifolder server url> --ifolder-id=<ID of the iFolder for which restore operation is performed> --ifolder-path=<Parent level path for actual data to be restored> --relative-path=<Relative path of file or folder to be restored>`

Common Use Case Scenarios

This section discusses some use case scenarios to help illustrate how to use the data recovery tool. For a list of caveats to be considered while using the tool, see "Caveats" on page 142.

- "Listing iFolders" on page 138
- "Restoring a Subfolder" on page 138
- "Restoring an iFolder" on page 139

Listing iFolders

Consider a scenario where a user named Bob wants to restore an iFolder named `mydocs`. However, Bob does not know the iFolder ID or the exact location of the folder.

To determine the actual location of the iFolder in the database and information such as the number of iFolders or the iFolder ID, the administrator can use the `--list` command:

```
ifolder-data-recovery --list –-path <temporary location where database content is restored> --backup-admin=<admin login name> --user=Bob
```

The output of this command lists all the iFolders, along with details such as the iFolder name, iFolder ID, and the path (the location where the iFolder is stored at).

Restoring a Subfolder

Files are restored from iFolder and its immediate subfolder. The subsequent subfolders cannot be restored. If you need to restore a folder down the level, ensure parent directory path is present.

Consider a scenario where a user named Bob has lost a folder named `mydocs/temp` from the `mydocs` iFolder.

1. Obtain information such as the user login ID, iFolder name, and subdirectory or file that needs to be restored.

   In this example, this would be: Bob (user ID), mydocs (iFolder name), and mydocs/temp (the directory to be restored).

2. Log in to the Web Admin console and click *User* > *Bob* > *mydocs*.

   Under the iFolder details you can find the iFolder path in the *path* field.

   The path can also be determined by using the `--list` command. For example, the iFolder path might be `/var/simias/data/simias/SimiasFiles/09/9b581fe2-e4d8-4178-8d8a-699db8118f13/mydocs`

3. Using a backup application, restore the iFolder database content to a temporary location, such as `/tmp/olddatabase/simias`.

4. From the backup, restore the actual iFolder content to the temporary location. For example, you would restore the actual iFolder content `/var/simias/data/simias/SimiasFiles/09/9b581fe2-e4d8-4178-8d8a-699db8118f13/mydocs` to a temporary location, such as `/tmp/iFolderdata/mydocs`.

5 Run the data recovery tool with the following options:

```
ifolder-data-recovery --restore --path <temporary location where database
content is restored> --backup-admin=admin --backup-password <password of the
backup admin> --current-admin=admin --current-password <password of the current
server's admin> --server-url=http://100.99.101.01 --ifolder-id= 9b581fe2-e4d8-
4178-8d8a-699db8118f13 --ifolder-path=<temporary location where ifolder
content is restored> --relative-path=mydocs/temp
```

Restoring an iFolder

Consider a scenario where a user named Bob has lost an iFolder named `mydocs`.

1 Obtain information such as the user login ID and the name of the iFolder that needs to be restored.

   In this example, this would be Bob (user ID) and mydocs (iFolder name).

2 Using a backup application, restore the iFolder database content to a temporary location, such as `/tmp/olddatabase`.

3 Run the `list` command to get the actual iFolder location:

```
/ifolder-data-recovery --list --path <temporary location where database content
is restored> --backup-admin=admin –user=Bob
```

4 Determine the actual iFolder content location from the output of the command in Step 3 and restore the iFolder from backup to a temporary location, such as `/tmp/iFolderdata/mydocs`.

5 Run the data recovery tool with the following options:

```
ifolder-data-recovery --restore --path <temporary location where database
content is restored> --backup-admin=admin --backup-password <password of the
backup admin> --current-admin=admin --current-password <password of the current
server's admin> --server-url=http://100.99.101.01 --ifolder-id=9b581fe2-e4d8-
4178-8d8a-699db8118f13 --ifolder-path=<temporary location where ifolder
content is restored>
```

Use Case Scenarios for Restoring Encrypted iFolders

When you use the data recovery tool to restore encrypted iFolders, the iFolders might not synchronize automatically after restoration and might display a message indicating `Incomplete Synchronization`.

- "The Encrypted iFolder Has the Same Passphrase and Recovery Agent as the Current Server" on page 140
- "The Encrypted iFolder Has a Different Passphrase and the Same Recovery Agent as the Current Server" on page 140
- "The Encrypted iFolder Has a Different Recovery Agent and the Same Passphrase as the Current Server" on page 140
- "The Encrypted iFolder Has an Unknown Passphrase and Has the Same Recovery Agent as the Current Server" on page 140
- "The Encrypted iFolder Has an Unknown Recovery Agent and Has the Same Passphrase as the Current Server" on page 141
- "The Encrypted iFolder Has an Unknown Recovery Agent and an Unknown Passphrase" on page 141

The Encrypted iFolder Has the Same Passphrase and Recovery Agent as the Current Server

If the restored encrypted iFolder has the same passphrase and Recovery agent as the current iFolder server, no further action is needed. After the restoration, iFolder starts synchronization as expected. However, for any *Merge* operation, you must resolve conflicts. For more information on resolving conflicts, see "Resolving File Conflicts" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

The Encrypted iFolder Has a Different Passphrase and the Same Recovery Agent as the Current Server

If the restored encrypted iFolder has a different passphrase but the same Recovery agent as the current iFolder server, then post restore, iFolder reports Incomplete Synchronization after the restoration. To have synchronization work as expected, you need to change the passphrase.

1. Access the Change Passphrase dialog box.

   For more information, see "Changing the Passphrase" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.
2. Specify the old passphrase in the *Enter passphrase* field.
3. Specify the passphrase for the current iFolder server in both the *Enter new* and *Retype passphrase* fields.
4. Select the current Recovery agent and perform the change passphrase operation.

The Encrypted iFolder Has a Different Recovery Agent and the Same Passphrase as the Current Server

If the restored encrypted iFolder has same passphrase as the current server but has a different Recovery agent, you need to change the Recovery agent.

1. Access the *Change Passphrase* dialog box.

   For more information, see "Changing the Passphrase" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.
2. Specify the old passphrase in *Enter passphrase* field.
3. Specify the passphrase for the current iFolder server in both the *Enter new* and *Retype passphrase* fields.
4. Select the current Recovery agent and perform the change passphrase operation.

The Encrypted iFolder Has an Unknown Passphrase and Has the Same Recovery Agent as the Current Server

If the restored encrypted iFolder has the same Recovery agent as the current server, but has a different passphrase and you don't know what the passphrase is, encrypted iFolders might not synchronize automatically after restoration and might display a message indicating Incomplete Synchronization.

If this happens, use the *Forgot Passphrase* option with the same Recovery agent and use the current server passphrase as new passphrase. For more information, see "Recovering an Encrypted iFolder " in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

The Encrypted iFolder Has an Unknown Recovery Agent and Has the Same Passphrase as the Current Server

If the restored encrypted iFolder has a different Recovery agent but has the same passphrase as the current server, and both the Recovery agent and passphrase are known, you must change both the passphrase and the Recovery agent:

1. Access the Change Passphrase dialog box.

   For more information, see "Changing the Passphrase" in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.
2. Specify the old passphrase in *Enter passphrase* field.
3. Specify the passphrase for the current iFolder server in both the *Enter new* and *Retype passphrase* fields.
4. Select the current Recovery agent and perform the change passphrase operation.

The Encrypted iFolder Has an Unknown Recovery Agent and an Unknown Passphrase

If the restored encrypted iFolder has a Recovery agent and passphrase that are different from the current server and both these values are unknown, the restored iFolder cannot be recovered.

Using Logs

The restore tool logs are located at: `<simias log location>/ifrecovery/`

The table given below summarizes the different types of log files:

Table 10-1 *iFolder Data Recovery Tool Logs*

Log Files	Description
<ifolderid>.failed	Contains information about all the entries that failed during the restore/retry operations.
debug.log	Contains all information pertaining to the execution of the tool.
<ifolderid>.notfound	Contains information about all the entries not found in the backup store during the restore/retry operations.
<ifolderid>.xml	Contains details such as the result of the last operation (successful/ failed), member details, and the relative path for the type of restore operation performed.
<ifolderid>.failedworking	Contains information about failed entries during a retry operation.

NOTE: If there is any failure in the last run of a particular iFolder restore operation, subsequent restore operation requests prompt for a retry. To perform a new restore operation, you must delete all files related to the iFolder ID from the log location.

Caveats

Consider the following caveats when you use the data recovery tool:

- The tool fails and exits gracefully if Apache is restarted. To continue the restore operation, use the `--retry` option.
- If an iFolder level restore operation fails (the tool exits in between operations), the iFolder might be shared with the administrative user of the system. In such a case, you should delete the partially restored iFolder, remove the old backup, remove all corresponding logs from the log location (logs such as <ifolderid>.xml, <ifolderid>.failed, <ifolderid>.notfound, <ifolderid>.working), and start `--restore` operation with a fresh backup.
- If you do a full iFolder restore, the tool restores/overwrites all the files and folders inside the iFolder that is to be restored. For example, assume that an iFolder has 10 files. You have lost 3 out of 10 files.If you restore the complete iFolder, all 10 files are restored instead of just the missing 3 files.
- If a filename is changed after the backup is taken and the file exists on the server at the time of the restore, only the content is restored and filename remains unchanged. However, if the file doesn't exist on the server at the time of the restore, the file is restored with the filename it had before the rename operation. For example, assume that a file named `a.txt` is renamed to `b.txt` after a backup is taken. If the `b.txt` file exists on the server during a restore, only the contents of the file are restored and the file name of the restored file remains as `b.txt`. However, if the `b.txt` file does not exist on the server, the file is restored as `a.txt`.
- If the tool does not start, run the `ps -ef | grep mono` command. Verify if a process is running on port 8086. If a process is running on port 8086, kill the running process and restart the tool. If a process is not running, make sure that the backup is not corrupted.

10.11 Changing The IP Address For iFolder Services

When you reconfigure the iFolder services, you must ensure that the current data Store path is not changed. Changing the IP address of the Novell iFolder service also needs the Apache service to be restarted. Follow the steps given below to change the IP address through CLI.

1. Open a terminal console and enter `rcapache2 stop`.
2. Run `/usr/bin/simias-server-setup`.
3. Specify the `Store path`.

   The default Store path is `/var/simias/data/simias`.
4. Specify the new Private IP address and Public IP address.

   IMPORTANT: Ensure that the users are notified about the new IP address for connection.
5. For the rest of the options, accept the default values because these values are from the existing configuration.
6. Start Apache service by executing `rcapache2 start`.

10.12 Securing Enterprise Server Communications

This section describes how to configure SSL traffic between the iFolder enterprise server and other components. HTTPS (SSL) encrypts information transmitted over shared IP networks and the Internet. It helps protect your sensitive information from data interception or tampering.

- Section 10.12.1, “Using SSL for Secure Communications,” on page 143
- Section 10.12.2, “Configuring the SSL Cipher Suites and Protocol for the Apache Server,” on page 143
- Section 10.12.3, “Configuring the Enterprise Server for SSL Communications with the LDAP Server,” on page 144
- Section 10.12.4, “Configuring the Enterprise Server for SSL Communications with the iFolder Client,” on page 144
- Section 10.12.5, “Configuring the Enterprise Server for SSL Communications with the Web Access Server and Web Admin Server,” on page 145
- Section 10.12.6, “Configuring an SSL Certificate for the Enterprise Server,” on page 145

For information about configuring SSL traffic for the iFolder Web access server, see Section 14.5, “Securing Web Access Server Communications,” on page 187.

10.12.1 Using SSL for Secure Communications

In a default deployment, the iFolder 3 enterprise server uses SSL 3.0 for secure communications between components as shown in the following table.

iFolder Component	Web Access Server	LDAP Server	Client	Web Browser
Enterprise Server	Yes	Yes	Yes	yes

iFolder uses the SSL 3.0 protocol instead of SSL 2.0 because it provides authentication, encryption, integrity, and non-repudiation services for network communications. During the SSL handshake, the server negotiates the cipher suite to use, establishes and shares a session key between client and server, authenticates the server to the user, and authenticates the user to the server.

The key exchange method defines how the shared secret symmetric cryptography key used for application data transfer will be agreed upon by client and server. SSL 2.0 uses only RSA key exchange, while SSL 3.0 supports a choice of key exchange algorithms, including the RC4 and RSA key exchange, when certificates are used, and Diffie-Hellman key exchange for exchanging keys without certificates and without prior communication between client and server. SSL 3.0 also supports certificate chains, which allows certificate messages to contain multiple certificates and support certificate hierarchies.

10.12.2 Configuring the SSL Cipher Suites and Protocol for the Apache Server

To ensure strong encryption, we strongly recommend the following configuration for the Apache server’s SSL cipher suite and protocol settings.

- Use only High and Medium security cipher suites, such as RC4 and RSA.

- Remove from consideration any ciphers that do not authenticate, such as Anonymous Diffie-Hellman (ADH) ciphers.
- Use TLS v1 and higher versions and disable SSL 2.0.
- Disable the Low, Export, and Null cipher suites.

To set these parameters, modify the aliases in the OpenSSL ciphers command (the SSLCipherSuite directive) in the `/etc/apache2/vhosts.d/vhost-ssl.conf` file.

1. Stop the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 stop
   ```

2. Open the `/etc/apache2/vhosts.d/vhost-ssl.conf` file in a text editor and do the following:

   2a Locate the SSLCipherSuite directive in the Virtual Hosts section and modify the plus (`+`) to a minus (`-`) in front of the ciphers you want to disable and make sure there is a `!` (not) before ADH:

   ```
   SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP:-eNULL
   ```

   2b Locate the SSLProtocol directive in the virtual hosts section and modify it include TLS v1:

   ```
   SSL Protocol TLSv1
   ```

3. Save your changes.
4. Start the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 start
   ```

For more information about configuring strong SSL/TLS security solutions, see SSL/TLS Strong Encryption: How-To (http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html) on the Apache.org Web site.

10.12.3 Configuring the Enterprise Server for SSL Communications with the LDAP Server

By default, the iFolder enterprise server is configured to communicate via SSL with the LDAP Server. For most deployments, this setting should not be changed. If the LDAP server is on the same machine as the enterprise server, communications do not need to be secured with SSL.

1. Log in to Web Admin.
2. Click *System* in the Web Admin console to open the System page.
3. Select *Enable SSL* to enable LDAP SSL communication.

10.12.4 Configuring the Enterprise Server for SSL Communications with the iFolder Client

By default, the iFolder enterprise server is configured to require SSL. If set to use SSL, all iFolder client communication to the server is encrypted using the SSL protocol. In most deployments, this setting should not be changed because iFolder uses HTTP BASIC for authentication, which means passwords are sent to the server in the clear. Without SSL encryption, the iFolder data is also sent in the clear.

1. Stop the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 stop
   ```

2 Go to `/usr/bin` and run `simias-server-setup`

3 Select `Yes` for the `Enable SSL` option.

4 Start Apache: At a terminal console, enter

```
/etc/init.d/apache2 start
```

10.12.5 Configuring the Enterprise Server for SSL Communications with the Web Access Server and Web Admin Server

By default, the Web Browser is configured to communicate via SSL with the iFolder Web Access server/ Web Admin server. The Web Access server/ Web Admin server communicate via SSL channels with the iFolder Enterprise Server. If the iFolder deployment is in a larger scale and the Web Access server or Web Admin server are on different machine than the iFolder enterprise server, then SSL enables you to increase the security between the two servers.

Communications between the two servers are governed by the Web Access server's or Web Admin server's settings for SSL traffic. For information, see Section 14.5.3, "Configuring the Web Access Server for SSL Communications with the Enterprise Server," on page 188.

10.12.6 Configuring an SSL Certificate for the Enterprise Server

For information, see "Managing SSL Certificates for Apache" on page 221.

11 Managing iFolder Services via Web Admin

This section discusses how to manage services for the Novell iFolder enterprise server using the iFolder Web Admin Console.

- Section 11.1, “Accessing the Novell iFolder Web Admin,” on page 147
- Section 11.2, “Connecting to the iFolder Server,” on page 147
- Section 11.3, “Managing Web Admin Console,” on page 149
- Section 11.4, “Managing the iFolder System,” on page 150
- Section 11.5, “Managing iFolder Servers,” on page 159
- Section 11.6, “Securing Web Admin Server Communications,” on page 166

11.1 Accessing the Novell iFolder Web Admin

Use the Novell iFolder Web Admin to manage the iFolder system, user accounts, and iFolders.

1. Open a Web browser to the following URL:

   `https://svrname.example.com/admin`

   Replace *`svrname.example.com`* with the actual DNS name or IP address (such as `192.168.1.1`) of the server where iFolder is running.

   IMPORTANT: The URL is case sensitive.

2. If prompted to verify the certificates, review the certificate information, then click *Yes* if it is valid.
3. On the iFolder Web Admin login page, enter the username and password in the *Username* and *Password* field and click the *Log In* button.

11.2 Connecting to the iFolder Server

Although you are logged in to iManager, you must provide the iFolder Administrator credentials to authenticate to the specific iFolder servers you want to manage. The iFolder Admin username can be the same LDAP identity as your iManager Admin username, depending on how you configure your iFolder system. Log in with the iFolder Admin username and password for the target server.

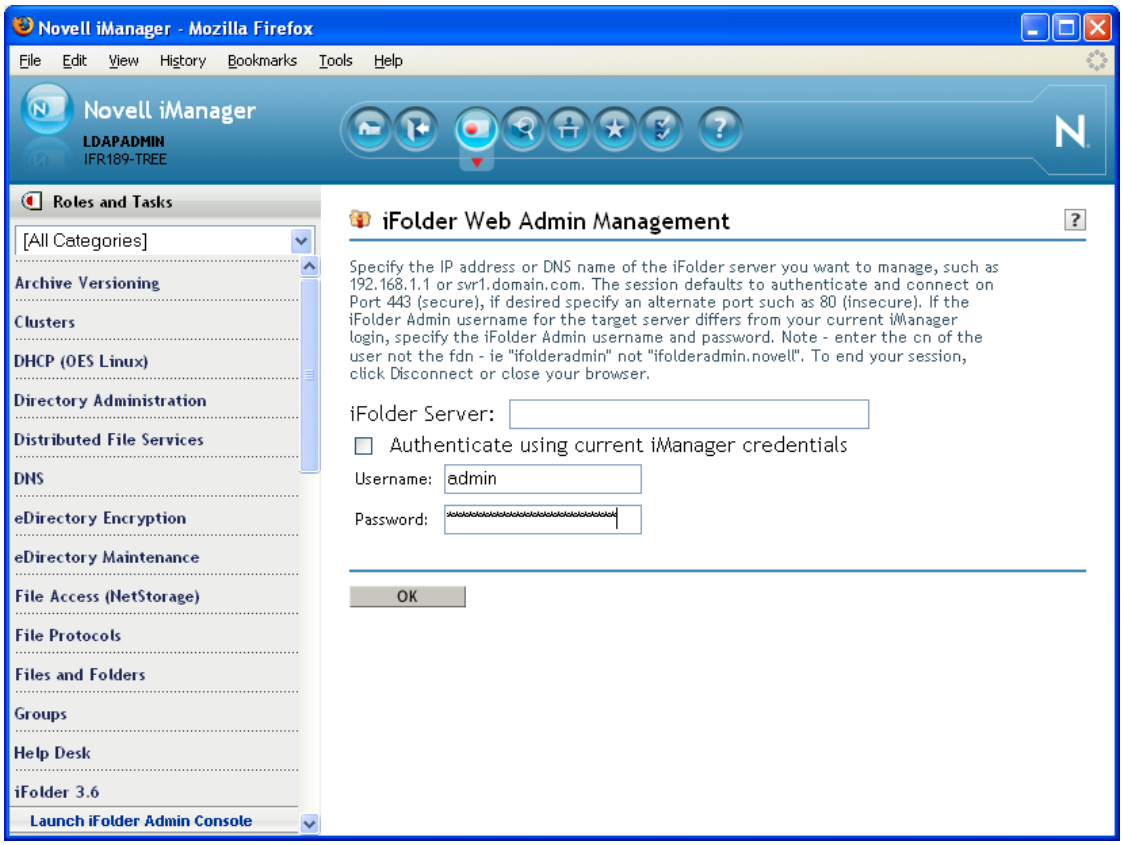
NOTE: You cannot manage Novell iFolder 2.*x* servers with the Novell iFolder 3 Web Admin.

To connect to the iFolder server you want manage:

1. If you are not logged in to iManager, log in to iManager in a Web browser.

   For information, see Section 11.1, “Accessing the Novell iFolder Web Admin,” on page 147.

2. In *Roles and Tasks*, expand the *iFolder 3.9* role and click *Launch iFolder Admin Console* to launch iFolder Web Admin Management page.



IMPORTANT: Web Admin console does not appear unless you disable the pop up blocker.

3 Specify the DNS name or IP address of the iFolder enterprise server you want to manager.

For example, type `svr1.example.com` or `192.168.1.1`.

4 Do one of the following:

- If you logged in to iManager with the same username as the iFolder Admin user of the target server, select *Authenticate Using Current iManager Credentials*.
- If you logged in to iManager with a different username than the iFolder Admin user of the target server, deselect *Authenticate Using Current iManager Credentials,* then specify the iFolder Admin username and password.

5 Click *OK* to connect to the iFolder server.

6 (Conditional) If prompted to accept the server's certificate, review the certificate information, then click *OK* to accept it if it is valid.

Based on the above selection, you are directed to the Web Admin users page.

7 Continue with Section 11.3, "Managing Web Admin Console," on page 149.

When you are done managing the iFolder server, click *logout* (located in the upper right corner) or close your Web browser to disconnect from the iFolder server you are managing. If you do not log out, the connection to the iFolder enterprise server remains open until your session times out, which can be a security risk.

11.3 Managing Web Admin Console

With Web Admin console you can manage iFolder users, LDAP Groups, the iFolder system, servers, iFolders, and the iFolder statistics report. In Web Admin console by default the *Users* page opens to the *Users* tab.

Users Page

NOTE: The term iFolder users refers to both individual users and LDAP Groups.

1. The *Users* tab displays the user's type (Admin user or user), username, user's full name (if available), the server to which the user is provisioned, and the user status (Enabled or Disabled).
2. Use the search functionality to locate the user whose iFolder account you want to manage.
3. Click the user's name link to open the User Details page.

   The User page opens to the Users tab, which displays the user details, iFolders owned, and shared and policy settings for this particular user account. For more information, see Chapter 12, "Managing iFolder Users," on page 169.

Accessing the iFolders Page

1. In the Web Admin console, click the *iFolders* tab.

   iFolders tab displays the iFolder type (Admin user or user), iFolder name, iFolder owner, members, the date the iFolder was last modified.
2. Use the search functionality to locate the iFolder you want to manage.
3. Click the iFolder's link to open the iFolder Details page to the iFolder tab.

   The iFolder Details page displays the iFolder details, list of members who own or share the iFolders and policy settings for this particular iFolder.

Accessing Systems Page

1. In the Web Admin console, click the *Systems* tab.

   The Systems page displays the system settings and list of iFolder Administrators.
2. Locate the iFolder Administrator you want to manage. You can add or delete iFolder Administrator.

   You can also manage the policy settings for the Admin user.
3. Click the Admin user's Name link to open the User Details page.

   The User Details page opens to the Users tab, which displays the user details, iFolders owned, and shared and policy settings for this particular user account. For more information, see Section 11.4.1, "Viewing and Modifying iFolder System Information," on page 150.

Accessing Servers Page

1. In the Web Admin console, click the *Servers* tab.
2. Use the search functionality to locate the Server you want to manage.

3 Click the Server name link to open the Servers Details page.

The Server Details page opens to the Servers tab, which displays server details, server status, server logs, and server reports, and to set the log level.

Accessing Reports Page

1 In the Web Admin console, click *Reports* tab.

2 Configure reporting according to the frequency and time schedule you want, then generate the output as desired.

11.4 Managing the iFolder System

This section discuss how to manage the iFolder services for a selected server.

- Section 11.4.1, “Viewing and Modifying iFolder System Information,” on page 150
- Section 11.4.2, “Viewing Reprovisioning Status,” on page 151
- Section 11.4.3, “Configuring iFolder Administrators,” on page 152
- Section 11.4.4, “Configuring System Policies,” on page 156

11.4.1 Viewing and Modifying iFolder System Information

In Web Admin Console, System page opens to the System tab to view and modify the following information:

Table 11-1 *System Information*

Parameter	Description
Name	The name assigned to the iFolder domain. To edit the name of the iFolder domain, enter the new name and click *Save*. To cancel the changes made, click *Cancel*.
Description	A short description about the iFolder Domain. To edit the system description, enter the new description and click Save. To cancel the changes made, click *Cancel*.
SSL Option	Displays the mode of communication between the iFolder Servers, iFolder Client, iFolder Web Access Console, and iFolder Web Admin Console.
Total Users (view only)	Reports the total number of users in the iFolder domain.
Total iFolders (view only)	Reports total number of iFolders that belongs to the iFolder domain.

Parameter	Description
Full Name Display Order	Enables you to set the order in which a user's full name is displayed. Select the *(First Name, Last Name)* option to display the first name followed by the last name. Or, to display the last name followed by the first name, select the *(Last Name, First Name)* option. For the changes to take effect, either a scheduled LDAP sync must take place or you must do a manual LDAP sync. To do a manual LDAP sync: 1. In the Web admin console, click the *Servers* tab, select the server, then go to the Serverdetails page. 2. In the LDAP Details section, click the *Sync Now* button.
Manage Group Quota Using	Enables you to define how the aggregate disk quota set for groups is managed. Select the *Administrator Console* option to enable administrators to explicitly manage the disk quota for groups and members of a group. When you select this option, the disk quota assigned to the users is restricted so that it does not exceed the aggregate disk usage of the group. By default, the Administrator Console option is selected. Select the *Sync Engine* option to enable the sync engine to manage the aggregate disk quota on groups in the back end. The sync engine ensures that the disk quota for all users in a group does not exceed the aggregate disk quota of the group. Select the *Both* option to use both the administrator console and the sync engine to manage the aggregate disk quota usage for groups.
Segregated Groups	Enables you to segregate groups into independent entities and ensure that members of one group are not accessible by members of another group for sharing iFolders. Select the *Create Segregated Groups* check box to enable sharing of iFolders only among the members of the same group.

11.4.2 Viewing Reprovisioning Status

You can move users across different servers. Click *Reprovision Status* to view the reprovisioning status for each user. You can view the following information:

Table 11-2 *Reprovisioning Status*

Parameter	Description
Type	indicates a provisioned user. indicates a unprovisioned user.
User Name	The username assigned to the user account, such as jsmith or john.smith@example.com.
Current Home	Shows the Home server assigned to a provisioned user.
New Home	Shows the new server to provision for the user.
Completed	Shows the reprovisioning status as a percentage.

Parameter	Description
Reprovision State	Shows any of the following reprovisioning states: ◆ Initializing ◆ Initialized ◆ Moving iFolder ◆ Resetting Home ◆ Finalizing

11.4.3 Configuring iFolder Administrators

This section discusses the following:

- "Multi-level administration" on page 152
- "Understanding the iFolder Admin User" on page 152
- "Viewing the Admin User Details" on page 153
- "Granting iFolder Admin Right to a User" on page 153
- "Removing the iFolder Admin Right for a User" on page 153
- "Understanding the secondary administrator" on page 154
- "Creating a secondary administrator" on page 154
- "Editing secondary administrator details" on page 156
- "Deleting secondary administrator" on page 156

Multi-level administration

Novell iFolder enables you to create multi-level administrators to manage your iFolder system. Using this feature you can create primary as well as secondary administrators. A primary administrator is also known as the iFolder admin user unless stated otherwise. The sections given below describe the iFolder admin user or the primary administrator and the secondary administrator.

Understanding the iFolder Admin User

The iFolder Admin user is the primary administrator of the iFolder enterprise server. Whenever iFolders are orphaned, the ownership of the orphaned iFolders is transferred to the iFolder Admin user. The iFolder admin user can then reassign the orphaned iFolders to another user or delete the iFolders.

The iFolder Admin user must be provisioned to enable the iFolder Admin to perform management tasks. iFolder tracks this user by the LDAP object GUID, allowing it to belong to any LDAP context in the tree, even those that are not identified as search contexts. The user's movement can be tracked anywhere in the tree because it is known by the GUID, not the user DN.

The iFolder Admin right can be assigned to other users so that they can also manage iFolder services for the selected server. Use the System tab of the Web Admin console to add or remove the iFolder Admin right for users. Only users who are in one of the contexts specified in the LDAP Search DN are eligible to be equivalent to the iFolder Admin user.

IMPORTANT: You cannot assign the Admin user right to an LDAP Group

If you assign the iFolder Admin right to other users, those users are governed by the iFolder user list and Search DN relationship. The user is removed from the user list and stripped of the iFolder Admin right if you delete the user, remove the user's context from the list of Search DNs, or move the user to a context that is not in the Search DNs.

Viewing the Admin User Details

The System page displays the following iFolder Admin details for the iFolder domain.

Table 11-3 *Admin User Details*

Parameter	Description
Type	Displays the Admin user icon.
User Name	The username assigned to the Admin user account, such as jsmith or john.smith@example.com.
Full Name	The first and last name of the Admin user account.

To view or edit Admin user details, click the Admin user link to open the User Details page. The User Details page displays the iFolders owned or shared by the user. Click the *All* tab to list all the iFolders, both owned and shared. To view the iFolder owned by the user, click the *Owned* tab. *Shared* tab lists all the shared iFolders for this particular user account. You can also change the policy settings for the selected Admin user.

Granting iFolder Admin Right to a User

You add the iFolder Admin right to one user at a time, but you can assign it to multiple users.

Repeat the following process for each user who you want to become an iFolder Admin user:

1. In the System page, click *Add* to open a list of iFolder Admin users.
2. Search for the user you want to grant Admin rights.
3. Select the *User* check box next to the user, then click *Add*.

   The username is added in the list of users with the iFolder Admin right. You can assign the iFolder Admin right to multiple users.

Removing the iFolder Admin Right for a User

You can delete the iFolder Admin right from all users in the list except the original iFolder Admin user.

IMPORTANT: You cannot delete the Admin user configured during simias server set-up.

If you delete the iFolder Admin right from the username you used to log in to the server, you are immediately disconnected. You must log in to the iFolder server under a different username with the iFolder Admin right to continue managing the server.

You remove the iFolder Admin right for one user at a time. Repeat the following process for each user who you want to remove as an iFolder Admin user:

1. In the *System* page, locate the Admin user you want to delete.
2. Click *Delete* to remove iFolder Admin right from the selected user.

Understanding the secondary administrator

A secondary administrator can only be created by a primary administrator. After creating a secondary administrator, the secondary administrator is assigned a group.

NOTE: Multiple groups can be managed by a single secondary administrator and a single group can be managed by multiple secondary administrators.

The secondary administrator can manage the group members based on the policy rights that are assigned to the secondary administrator. These policy rights are set by the primary administrator. The policy rights govern the policies that the secondary administrator can set for the group members. For instance, if the *iFolders per user* policy is enabled for a secondary administrator, this means that the secondary administrator can set the *iFolders per user* policy for the group members.

Creating a secondary administrator

To create a secondary administrator, follow the steps given below:

1. In the *System* page, click the *Secondary Administrator* tab and then click *Add* to display the list of iFolder users.
2. Select the user that you want to designate as a secondary administrator and click *Next*.
3. To assign a group to the secondary administrator, select an option from the *Select Group* list.
4. Set the aggregate disk quota for a group by specifying a value in the *Set the Aggregate Disk Quota Limit For Entire Group* field.

   NOTE: If the selected group has the aggregate disk quota limit already set, then *Set the Aggregate Disk Quota Limit For Entire Group* field is populated with that value. Otherwise, the field will remain empty.

   ---

5. Set the policy rights for the secondary administrator.

   The following table lists the policy rights that you can set for the secondary administrator.

   Table 11-4 *Secondary Administrator Policies*

Parameter	Description
iFolder Per User Policy	Specifies the maximum number of iFolders allowed per user. After you apply this policy, each user is limited to owning a certain number of iFolders. The users who exceed the limit receive an error message about the policy violation. If the limit is zero, users cannot create any iFolders. This policy setting does not affect the number of iFolders a user already owns. If the number of iFolders owned by a user already exceeds the limit that you set, the user can still own those iFolders. By default, the *Allow* check box is selected for the iFolder Per User policy. This means that the secondary administrator has the right to set the iFolder per user policy for the users of the designated group. To deny this right to the secondary administrator, you must deselect the *Allow* check box.

Parameter	Description
Disk Quota Policy	Specifies the maximum space that a user is allowed to use. By default, the *Allow* check box is selected for the disk quota policy. This means that the secondary administrator has the right to set the disk quota policy for users of the designated group. To deny this right to the secondary administrator, you must deselect the *Allow* check box.
File Size Policy	Specifies the maximum file size that can be synchronized. By default, the *Allow* check box is selected for the file size policy. This means that the secondary administrator has the right to set the file size policy for users of the designated group. To deny this right to the secondary administrator, you must clear the *Allow* check box.
Sync Interval Policy	Specifies the minimum synchronization interval in minutes. By default, the *Allow* check box is selected for the sync interval policy. This means that the secondary administrator has the right to set the sync interval policy for users of the designated group. To deny this right to the secondary administrator, you must deselect the *Allow* check box.
Excluded File List Policy	Specifies the file types that are restricted from synchronization. By default, the *Allow* check box is selected for the excluded file list policy. This means that the secondary administrator has the right to set the excluded file list policy for users of the designated group. To deny this right to the secondary administrator, you must deselect the *Allow* check box.
Sharing	Specifies if iFolders can be shared among users. By default, *Allow to modify sharing policy* check box is selected for the sharing policy. This implies that the secondary administrator has the right to modify the sharing policy for users of the designated group. To deny this right to the secondary administrator, you must clear the *Allow* check box.
Encryption Policy	Specifies the encryption policy for the iFolder system. By default, *Allow to modify encryption policy* check box is selected for the encryption policy. This means that the secondary administrator has the right to modify the encryption policy for users of the designated group. To deny this right to the secondary administrator, you must deselect the *Allow* check box.
Provisioning Rights	Specifies the provisioning rights available to a secondary administrator. By default, the *Allow user provisioning* check box is selected. This means that a secondary administrator can provision the users of the designated group to any server present in the iFolder multi server setup. To deny this right to the secondary administrator, deselect the *Allow user provisioning* check box. By using the *Allow enabling/disabling of users* check box, you can assign the secondary administrator the right to enable or disable users of the designated group. By default, this check box is selected. To deny the secondary administrator this right, deselect the *Allow enabling/disabling of users* check box.

Parameter	Description
Rights on iFolders	Specifies the secondary administrator's rights on ifolders owned by users of the designated group. To allow the secondary administrator to own orphaned iFolders, ensure that the *Allow ownership of orphaned iFolders* check box is selected. By default this check box is selected. To deny this right to the secondary administrator, clear the check box. Using the *Allow Enabling/Disabling of iFolders* check box, you can assign the secondary administrator the right to enable or disable the iFolders owned by users of the designated group. By default, this check box is selected. To deny this right to the secondary administrator, clear the *Allow Enabling/Disabling of iFolders* check box. Using the *Allow to modify rights of shared iFolder members* check box, you can assign the secondary administrator the right to modify the rights of shared iFolder members. By default this check box is selected. To deny this right to the secondary administrator, clear the *Allow to modify rights of shared iFolder members* check box.

6 Click the *Save* button to save your settings.

7 After successfully assigning a group to the secondary administrator, click *OK* to return to the Systems page or click *Repeat* to assign more groups to the secondary administrator.

Editing secondary administrator details

To edit the secondary administrator details, follow the steps given below:

1 Click the *Secondary* tab to display the secondary administrator details.

2 Select a secondary administrator and click *Edit* to display the list of groups monitored by the secondary administrator.

3 Select a group and click *Edit* to display the list of secondary administrator's rights on the group. Edit the rights of the group and click *Save* to save your changes.

Deleting secondary administrator

To delete a secondary administrator, follow the steps given below:

1 Click the *Secondary* tab to display the secondary administrator details.

2 Select a secondary administrator and click *Delete* to display the list of groups monitored by the secondary administrator.

3 Select all groups and click *Delete*. Deleting all groups owned by the secondary administrator also deletes the secondary administrator.

11.4.4 Configuring System Policies

Use the System Policies page to manage system-wide policies.

Viewing the Current System Policies

The following table lists the system policies you can manage for any given iFolder System. Click *Save* to apply the modifications.

Table 11-5 *System Policies*

Parameter	Description
No of iFolders per users	Specifies the maximum number of iFolder allowed per user. After Applying this policy, each user is limited to own a certain number of iFolders. The users who exceed their limit receive an error message about the policy violation. If the limit is zero, users cannot create any iFolders. The policy setting does not affect the number of iFolder a user already owns. If the number of iFolders owned by a user already exceeds the limit that you set, he or she can still own those iFolders
Disk Quotas	The total combined administrative size (in MB) of space allocated for use by all iFolder users on this system. The administrative total can exceed the actual physical size of the system disks. Space is assigned as needed; it is not reserved.
File Size	Specifies the maximum file size (in MB) that iFolder system is allowed to synchronize.
Excluded Files	Specifies a list of file types to include or to exclude from synchronization for all iFolders on the system. You can use wildcard characters (such as "*", "?") with the file types. For example, to block all files with `mp3` extension, you need to specify `*.mp3`.
Synchronization	If this option is enabled, specifies the minimum interval (in minutes) for synchronizing iFolder data for the system. Larger values are more restrictive. If the option is disabled, the value is No Limit. The interval timer is reset to the Synchronization Interval value at the end of a synchronization session. When the time elapses, another session is started.
Encryption	Specifies the encryption policy for the iFolder system. System-wide settings supersede user policies.
Sharing	Specifies the sharing policy for the iFolder system. System-wide settings supersede user policies.

Modifying iFolder System Policies

1. Select the policy, specify values for the policy, then click *Save* to apply it:

Click *Cancel* to cancel the changes.

Parameter	Description
No of iFolders per users	Specifies the maximum number of iFolder allowed per user. After Applying this policy, each user is limited to own a certain number of iFolders. The users who exceed their limit receive an error message about the policy violation. If the limit is zero, users cannot create any iFolders. The policy setting does not affect the number of iFolder a user already owns. If the number of iFolders owned by a user already exceeds the limit that you set, he or she can still own those iFolders
Disk Quota	Select the check box to enable a system-wide quota, then specify the total space quota (in MB) for the current iFolder domain. Deselect the check box to disable a system-wide quota. If you enable a system-wide quota that is less than a user's current total space for iFolder data, the user's data stops synchronizing until the data is decreased below the limit or until the quota is increased to a value that is larger than the user's total space consumed. Enabling or modifying the system-wide quota does not affect existing individual user quotas. Any existing user quota always overrides system-wide quota, whether the user quota is lower or higher than the system-wide quota. Default value: 100 MB
File Size	Deselect the check box to disable the Maximum File Size Limit policy. If the policy is disabled, the value is reported as No Limit. Select the check box to enable the Maximum File Size Limit policy, then specify the maximum allowed file size in MB. Consider the following demands on your system to determine an appropriate file size limit for iFolders in your environment: ◆ Intended use ◆ How often the largest files are modified ◆ How the applications that use the largest files actually save changes to the file (whole file or deltas) ◆ How frequently the files are synchronized by each member ◆ How many users share an iFolder ◆ Whether users access iFolder on the local network or across WAN or Internet connections ◆ The average and peak available bandwidth Even if you set a very large value as a file size limit and if there is no quota to limit file sizes, the practical limit is governed by the file system on the user's computer. For example, FAT32 volumes have a maximum file size of 4 GB minus 1 byte. Default value: Disabled, No Limit

Parameter	Description
Excluded Files	Specify whether to restrict file types that are synchronized by exclusion filters. Type a file extension, then click *Add* to add it to the list. You can only add or delete file extensions; subsequent editing is not allowed on the entries.
Synchronization	To enable a policy, select the check box, then specify the minimum synchronization interval in minutes. For example, a practical value is 600 seconds (10 minutes). Larger values are more restrictive. To disable the policy, deselect the check box. The value is reported as No Limit. Default value: Disabled The effective minimum synchronization interval is always the largest value of the following settings: ◆ The system policy (default of zero), unless there is a user policy set. If a user policy is set, the user policy overrides the system policy, whether the user policy is larger or smaller in value. ◆ The local machine policy, or the setting on the client machine synchronizing with the server. ◆ The iFolder (collection) policy.
Encryption	Select *On* to enable the encryption feature for the iFolder system. This permits a user to set an encryption policy for his or her iFolders. Select *Enforced* to enable the encryption feature for all users. When it is set to Enforced, a user cannot change the encryption settings for his or her iFolders.
Sharing	**On:** By default, iFolder sharing is enabled. Select *On* to disable sharing for the iFolder system. After applying this policy, users of this iFolder system cannot share his or her iFolders with others. However, you can change the policy settings at the user level for any selected user. **Enforce:** You can enforce both enable sharing and disable sharing. When you enforce disable sharing, policy settings for sharing at iFolder and User level are automatically disabled and you are not allowed to change the settings. However, you are allowed to set the policy for *Revoke* option. **Revoke:** Select *Revoke* to remove the shared members of all the iFolders under the iFolder system.

11.5 Managing iFolder Servers

This section describes how to manage a iFolder server for a multi-server setup.

IMPORTANT: You cannot change the settings of any server from the Web Admin page of a different server.

- Section 11.5.1, “Searching For Servers,” on page 160
- Section 11.5.2, “Upgrading a Slave Server to a Master Server,” on page 165

11.5.1 Searching For Servers

The search functionality help you locate the server you want to manage.

1. In Web Admin, ensure that you are on Servers page.

   If you are not, click the Servers tab to open the Servers page.
2. Select a filter criterion (Contains, Begins With, Ends With, Equals).
3. Use one or more of the following search methods, then click Search:
   - Type the name of the server in the *Search Servers* field.
   - Type one or more letters in the *Search Servers* field.
   - Type an asterisk (*) in the *Search Servers* field to return a list of all Servers on the system.
   - Leave the *Search Servers* field empty to return a list of all Servers on the system.

Do not click anywhere in the page until the page completely refreshes, then you can browse, sort, or manage the servers listed in the Search Results report.

Scroll up and down to browse the search results and locate the Server you want to manage.

Accessing and Viewing the Server Details Page

Follow the steps given below:

1. On the Server page, use the search functionality to locate the server.
2. Click the Server's name link to open the Server Details page to the Servers page.
3. View the following server informations:

Parameter	Description
Name	The name assigned to the iFolder enterprise server.
Type	The host portion of the DNS name of the server. For example, in `if3svr.example.com`, `if3svr` is the host name.
DNS Name	The DNS name of the iFolder Enterprise server. For example: *192.168.1.1* or *svr1.domain.com*
Public URL	The public IP address corresponding to the iFolder server. To change the IP address, edit the address given and click *Save* to save the changes you have done.
Private URL	The private URL corresponding to the iFolder server. This allows communication between the servers within the iFolder domain. The private URL and the public URL can be the same. To change the IP address, edit the address given and click *Save* to save the changes you have done.
Master URL (Displayed only for Slave servers)	The IP address corresponding to the iFolder server. Using this address, slave server communicate with the master server in the iFolder domain. To change the IP address, edit the address given and click *Save* to save the changes you have done.

4. Select the report from the drop down list to view the detailed statistics about the user activities.

This option is disabled if the Enable Reporting option on the Report page is left unselected.

5 View the following server log information:

Parameter	Description
System	Select System to view the `simias.log` that tracks all the system activities.
User Access	Select User Access to view `simias.access.log` that tracks the user activities on the selected server.

6 Set the log level information for the *System* or for each *User access*.

6a Select the option from the drop-down list for which you want to set the log level information.

System is selected by default.

6b Click View to view the log level information.

Either you can save it to the machine or open with a desired file format.

Parameter	Description
All	Shows all the server activities that help Novell support resolve the issues.
Debug	Shows the server activities that help Novell support debug the issues. .
Info	Shows the basic server activities that help Novell support resolve the issues. This option is selected by default.
Warn	Shows all the potential system errors.
Error	Shows all the system errors that halt system functioning.
Fatal	Shows the fatal system errors.
Off	Logging is turned off.

7 Set the LDAP Details:

7a You can edit the following LDAP related information. Click *Save* to modify the entries. Click *Cancel* to cancel your modifications.

Parameter	Description
Up since	Shows the date and time of the very first synchronization.
Status	Reports the current LDAP sync engine status.
Cycles	Shows the number of times the synchronization take place.
Identity Sync	Updates iFolder users in the selected iFolder domain from the LDAP information at the interval you select. Specify the time interval in minutes in the Identity Sync field and click *Sync Now* to start synchronizing iFolder users with the LDAP users.

Parameter	Description
Delete member grace interval	Specifies the time interval for the iFolder to remove the user information completely from the iFolder server after the user is deleted from LDAP. For example, if you specify 10 minutes as *Delete member grace interval*, iFolder removes all the user information 10 minutes after the deletion of the user from the LDAP or after the change in LDAP context. However, you can recover all the user data within the specified period. Whenever an LDAP context is changed or some user are deleted from the LDAP context, irrespective of the current grace interval period, the first LDAP sync disables the users. The first LDAP sync can be manual by using the *Sync Now* button, or be scheduled. After the grace interval period, any scheduled or manual LDAP sync removes all the users from iFolder domain and all the user iFolders become orphans. Disabled users are never deleted automatically after the grace interval period. The users continue to exist in a disabled state even after the grace interval period until the next LDAP sync cycle. If the users are again created in the LDAP context or the removed context is configured again within the grace interval period, the user becomes active with all the iFolders. However, the user remains in a disabled state. You can enable the user from the Web Admin console. For more information, see Section 12.5, "Enabling and Disabling iFolder User Accounts," on page 176.
LDAP Context	Lists all the LDAP contexts. iFolder searches users only from the listed LDAP contexts.

7b You can edit the following LDAP related information. Click *Edit* to open a new page where you can modify the entries. You must be authenticated to the LDAP server before you can edit the entries.

Parameter	Description
LDAP Server	Shows LDAP Server address.
LDAP SSL	Allow you to enable or disable LDAP SSL connection.
Proxy User	The iFolder Proxy user is the identity used to access the LDAP server to retrieve lists of users in the specified containers, groups, or users that are defined in the iFolder LDAP settings. This identity must have the Read right to the LDAP directory. The iFolder Proxy user is created during the iFolder install.
Proxy User Password	The password is used to authenticate the iFolder Proxy user to the LDAP server when iFolder synchronizes users with the LDAP server. **NOTE:** If iFolder is configured to use OES common proxy, then the proxy user password must not be changed from iFolder Web Admin console.
LDAP Context	Lists all the LDAP contexts. iFolder searches users only from the listed LDAP contexts.

7c Authenticate to the LDAP server and modify the LDAP Details, then click *OK* to apply your changes:

Parameter	Description
LDAP Admin DN	Specify the fully distinguished name of the LDAP Admin. This might be the same or different as your iFolder Admin.
LDAP Admin Password	The password is used to authenticate the LDAP Admin user to the LDAP server.Click *OK* to update the password stored in the LDAP settings.
LDAP Server	Specify the DNS name or IP address of the LDAP server. This might be the same or a different server as any of the iFolder servers in the iFolder system.
LDAP SSL	Select Yes to enable LDAP SSL. If SSL is enabled on the server, the value is *Yes*; otherwise, the value is *No*.
Proxy User	The iFolder Proxy user is an existing proxy user identity used to access the LDAP server with Read access to retrieve a list of authorized users. The proxy user is automatically created during the iFolder enterprise server configuration. The username is auto-generated to be unique on the system. Make sure that the user account assigned as the iFolder Proxy user is different than the one used for the iFolder Admin user and other system users. Separating the proxy user from the administrator provides privilege separation and is also important because the proxy user password is stored in the file system on the iFolder server. Specify the fully distinguished name of an existing user that you want to make the iFolder Proxy user. This identity must have the Read right to the LDAP directory. For example: cn=iFolderProxy,o=acme Make sure to also enter the new user's password in the Proxy Password field. After you modify the Proxy user, you might want to immediately synchronize the LDAP user lists, using the new iFolder proxy information; otherwise, it is not tested until the next scheduled synchronization of the user list. Use the *Sync Now* option under LDAP Details on the Server Details page to synchronize the iFolder user list on demand and verify your new Proxy user settings.
Proxy User Password	To modify the iFolder Proxy User password, you can directly use this interface to modify the password.This password must match the password stored in the iFolder Proxy user’s eDirectoryTM object.Specify the password twice, then click *OK* to update the password stored in the LDAP settings.

Parameter	Description
LDAP Context	Specify or edit the LDAP containers, groups, or users where iFolder searches for a list of authorized users to provision for iFolder servers on this enterprise server. LDAP Contexts are entered in LDAP format. For example: cn=group,o=acme#cn=dbgroup,o=acme# To edit a value, select it, make your changes, then click OK to apply the changes. During LDAP synchronization, the iFolder server queries the LDAP server to retrieve a list of users in the DNs (as specified in the LDAP Contexts field) at the specified synchronization interval. The usernames in the iFolder domain are matched against this official LDAP list. Any new user in the specified LDAP contexts are added to the iFolder domain. If a user is no longer in the specified LDAP contexts, the username is removed from the domain, any iFolders the user owns are orphaned and reassigned to the iFolder Admin user, and the user is removed as a member of other iFolders. The iFolder Admin User is provisioned for servers during the install. It is tracked by its GUID, so it is available even if you do not specify a container, group, or user, or if you specify Search DNs that do not contain the Folder Admin user. This identity must be provisioned to enable the iFolder Admin to perform management tasks.

8 Manage the Data store.

Data Store represents the iFolder storage that can span across multiple volumes (mount points) in a given server. By default, every iFolder server has a default store which cannot be disabled. With web interface, you can add and configure multiple Data Stores across which iFolder data is load balanced. When a user uploads an iFolder, it checks for the Data Store with maximum free space, and stores the iFolder data in that particular Data Store thereby balancing the load. You can add as many Data Stores as you want. Having multiple Data Stores thus makes it possible to scale the data storage capacity in a large deployment to meet the enterprise-level requirements.

You can view the following data store information:

Parameter	Description
Name	Shows the unique name you have specified for the Data Store.
Full Path	Shows the path to the Data Store, where the volume is mounted on. This is the data path that you have specified while adding the data store using the web interface.
Free Space	Shows the space available in the volume.
Enabled	Shows the given Data Store is enabled or not. Default Data Store cannot be disabled.

Deleting a Data Store: You can delete a Data Store if no iFolder is created on it. To delete a Data Store, select the check box next to that Data Store and click *Delete*.

Enable or Disable Data Store: Select the Data Store you want to disable or enable and click Disable or Enable respectively. When the user uploads an iFolder, disabled Data Stores are always skipped while checking for the maximum free space availability for storing the iFolder data.

To add a new Data Store,

8a Specify the following information:

Name: Assign a unique name to the Data Store, such as ifolder-store.

Path: Enter the path where the new volume is mounted. If it is a remote volume (CIFS, NFS, AFP), then ensure that the volume is mounted on every restart for proper functioning and load balancing. You need to check the permissions of the path specified, and change the ownership to Apache-user (wwwrun). Unless you have set the permission for the directory on to which the volume is mounted, you cannot create or sync iFolders on this volume.

Accessing and Viewing the Report Page

Use this interface to enable reporting and generate reports for iFolder and Directories.

It generate reports based on the frequency you select.

1. Select Enable Reporting to enable reporting.
2. Select the frequency from the given options (Daily, Weekly, Monthly).
3. Select the time when you want to generate the report.
4. Select the output option from the given options (Report iFolder, Report Directories)
5. Select the format for generating the report.
6. Click *Save* to save the settings.

   Click *Cancel* to cancel the settings.

11.5.2 Upgrading a Slave Server to a Master Server

In a multi-server (master-slave) setup, you may be required to upgrade a slave server to a master server based on your needs. For instance, consider a scenario where you have a master-slave configuration and the hardware on your master server is outdated. You have a slave server with high-end configuration that you would like to be a master server. iFolder enables you to upgrade a slave server to be a master server. On upgrading the slave server to a master server, the following changes take effect:

- The previous master server is designated as a slave server.
- All the slave servers in the multi-server setup are updated with new master information. If the slave servers are not updated with new master information, you must update the `simias.config` file with master server URL and restart the servers.

NOTE: To upgrade a slave server to a master server, all servers in the multi-server setup must be running the same version of iFolder.

All activities pertaining to the upgrade process are logged in the `simias.log` and `adminweb.log` files. You can upgrade a slave server to a master server using the Web Admin console.

1. In the Web Admin console, click the *Servers* tab.
2. Click the server that you want to upgrade to display the Server Details page.
3. Click *Set as Master* to designate the server as a master server.

After performing the above steps, it is recommended that you re provision the iFolder admin user to the new master server. For more information on re provisioning users, see Section 12.1.2, "Manual Reprovisioning," on page 170.

11.6 Securing Web Admin Server Communications

This section describes how to configure SSL traffic between the iFolder Web Admin server and other components. HTTPS (SSL) encrypts information transmitted over shared IP networks and the Internet. It helps protect your sensitive information from data interception or tampering.

11.6.1 Using SSL for Secure Communications

In a default deployment, the iFolder server uses SSL 3.0 for secure communications between components as shown in the following table.

Table 11-6 *SSL 3.0 for Secure Communication*

iFolder Component	Enterprise Server	LDAP Server	Client	Web Browser
Web Admin Server	Yes	Yes	Yes	Yes

For more information about SSL 3.0, see Section 10.12.1, "Using SSL for Secure Communications," on page 143.

11.6.2 Configuring the SSL Cipher Suites for the Apache Server

To restrict connections to SSL 3.0 and to ensure strong encryption, we strongly recommend the following configuration for the Apache server's SSL cipher suite settings.

- Use only High and Medium security cipher suites, such as RC4 and RSA.
- Remove from consideration any ciphers that do not authenticate, such as Anonymous Diffie-Hellman (ADH) ciphers.
- Use SSL 3.0, and disable SSL 2.0.
- Disable the Low, Export, and Null cipher suites.

To set these parameters, modify the aliases in the OpenSSL ciphers command (the SSLCipherSuite directive) in the `/etc/apache2/vhosts.d/vhost-ssl.conf` file.

1. Stop the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 stop
   ```

2. Open the `/etc/apache2/vhosts.d/vhost-ssl.conf` file in a text editor, then locate the SSLCipherSuite directive in the Virtual Hosts section:

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

3 Modify the plus (+) to a minus (-) in front of the ciphers you want to disable and make sure there is a ! (not) before ADH:

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP:-eNULL
```

4 Save your changes.

5 Start the Apache server: At a terminal console, enter

```
/etc/init.d/apache2 start
```

For more information about configuring strong SSL/TLS security solutions, see SSL/TLS Strong Encryption: How-To (http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html) on the Apache.org Web site.

11.6.3 Configuring the Web Admin Server for SSL Communications with the Enterprise Server

By default, the Web Browser is configured to communicate with the iFolder Web Admin server and the iFolder Enterprise server via SSL. If the iFolder deployment is in a large scale and the Web Admin server is on a different machine than the iFolder enterprise server, then SSL enables you to increase the security for communications between the two servers.

The communication between the Web Admin server and the iFolder enterprise server is determined during the configuration of the Web Admin server. Specify an https:// in the URL for the enterprise server for SSL (HTTPS) communications between the servers. Traffic between the two servers is secure. If you specify an http:// in the URL, HTTP is used for communications between the servers and traffic is insecure.

The setting is stored in the `/usr/lib/simias/webAdmin/Web.config` file under the following tag:

```
<add   key="SimiasUrl" value="https://localhost"   />
<add key="SimiasCert" value=<raw certificate data in base 64 encoding>   />
```

If you disable SSL between Web Admin server and the enterprise server and if the two servers are on different machines, you must also disable the iFolder server SSL requirement. Because the enterprise SSL setting also controls the traffic between the enterprise server and the client, all Web traffic between servers and between the clients and the enterprise server would be insecure.

IMPORTANT: Do not disable SSL on the Web Admin server if the servers are on different machines.

If the two servers are running on the same machine and you want to disable SSL, rerun the YaST configuration, and specify `http://localhost` as the URL for the enterprise server.

11.6.4 Configuring the Web Admin Server for SSL Communications with Web Browsers

The SSL connection supports the secure exchange of data. For most deployments, this setting should not be changed because iFolder uses HTTP BASIC for authentication, which means passwords are sent to the server in the clear. Without SSL encryption, the iFolder data is also sent in the clear.

The following Rewrite parameters control this behavior and are located in the `/etc/apache2/conf.d/ifolder_web.conf` file:

```
LoadModule rewrite_module /usr/lib/apache2/mod_rewrite.so

RewriteEngine On

RewriteCond %{HTTPS} !=on

RewriteRule ^/ifolder/(.*) https://%{SERVER_NAME}/ifolder/$1 [R,L]
```

To disable the requirement for SSL connections, you can comment out these Rewrite command lines in the `ifolder_web.conf` file. Placing a pound sign (`#`) at the beginning of each line renders it as a comment.

WARNING: Without an SSL connection, traffic between a user's Web browser and the Web Admin server is not secure.

To disable the SSL requirement:

1. Stop the iFolder Web Admin services.
2. Edit the `/etc/apache2/conf.d/ifolder_web.conf` file to comment out the Rewrite command lines.

   For example:

   ```
   #LoadModule rewrite_module /usr/lib/apache2/mod_rewrite.so

   #RewriteEngine On

   #RewriteCond %{HTTPS} !=on

   #RewriteRule ^/ifolder/(.*) https://%{SERVER_NAME}/ifolder/$1 [R,L]
   ```
3. Start the iFolder Web Admin services.

11.6.5 Configuring an SSL Certificate for the Web Admin Server

For information, see "Managing SSL Certificates for Apache" on page 221.

12 Managing iFolder Users

This section discusses how to manage iFolder users with Novell iFolder enterprise server.

- Section 12.1, “Provisioning / Reprovisioning Users and LDAP Groups for iFolder,” on page 169
- Section 12.2, “Searching for a User Account,” on page 170
- Section 12.3, “Accessing And Viewing General User Account Information,” on page 171
- Section 12.4, “Configuring User Account Policies,” on page 172
- Section 12.5, “Enabling and Disabling iFolder User Accounts,” on page 176

12.1 Provisioning / Reprovisioning Users and LDAP Groups for iFolder

In a multi-server environment, each user or LDAP Group member is provisioned to a home server when he or she logs in to the iFolder for the first time. When a user logs in for the first time, iFolder checks whether the user is already provisioned to a server manually.

If manual provisioning is not done, iFolder checks whether the user is provisioned to a server as specified in the LDAP attribute. It checks whether the LDAP home server attribute is set for the user or any of the user's LDAP Groups. If LDAP home server attribute is set, user is provisioned based on that.

If all of the above cases fail to provision the user, iFolder automatically select a server in the iFolder system and provision to the user on a round-robin basis.

NOTE: Provisioning a user or an LDAP Group to a slave server does not reflect immediately in the Web Admin console of the slave server. This is because you have done the provisioning at the Master server-level. The slave server receives the data only after a minimum of 30 seconds depending upon the network load and the Master server load for it to reflect in the Web Admin console of the slave server.

- Section 12.1.1, “Manual Provisioning,” on page 169
- Section 12.1.2, “Manual Reprovisioning,” on page 170
- Section 12.1.3, “Round-Robin Provisioning,” on page 170

12.1.1 Manual Provisioning

Use the iFolder Web Admin console to provision users for iFolder servers.

1. Log in to the iFolder Web Admin console and open *Users* page.
2. Do either of the following:
   - Locate and select the user, select the server from the drop-down list, then click *Save*.
   - Locate and select the users, then click *Provision* to open a new page. From the drop-down list in the new page, select the server and click *Provision/Reprovision*.

12.1.2 Manual Reprovisioning

With reprovisioning functionality, you can reassign a new server to an already provisioned user. Thus, you can manually move the users across different servers in any given iFolder domain.

NOTE: The user move must be initiated from the server it is provisioned to. For example, iFolder system has 2 servers OES 2 SP3 and OES 11 SP1. A user is provisioned to OES 2 SP3 server and needs to be moved to OES 11 SP1 server. Ensure to perform the user move task from the OES 2 SP3 server.

---

1. Log in to the iFolder Web Admin console and open *Users* page.
2. Perform the following:
   - Locate and select the users, then click *Provision* to open a new page. From the drop-down list in the new page, select the new server and click *Provision / Reprovision*.

12.1.3 Round-Robin Provisioning

If users and LDAP Groups are not provisioned either through the LDAP attribute or manually, they are automatically provisioned to iFolder servers on a round-robin basis. When a new user or member of an LDAP Group logs in to iFolder for the first time, iFolder checks for the server with the fewest number of users provisioned to it, and provisions the user to that server.

For example, suppose your iFolder system has three servers named `server A`, `server B` and `server C` and each server has users provisioned to it. If `server A` has 10 users, `server B` has 5 users, and `server C` has 12 users and a new iFolder user joins, the user is automatically provisioned to `server B,` which has the fewest users. Provisioning users to `server B` continues until it has 10 users, which is equal to the number of users provisioned to `server A,` so that `server B` gets the next new user. When all the three servers are provisioned with an equal number of users, the next new user is provisioned to any of these servers.

12.2 Searching for a User Account

NOTE: The term iFolder users refers to both individual users and LDAP Groups.

---

1. In Web Admin console, enable the *Users* tab.
2. Select a name criterion (*User Name*, *First Name*, *Last Name, Home Server*).
3. Select a filter criterion (*Contains*, *Begins With*, *Ends With*, *Equals*).
4. Use one or more of the following search methods, then click *Search*:
   - Type the name of the user in the *Search Users* field.
   - Type one or more letters in the *Search Users* field.
   - Type an asterisk (`*`) in the *Search Users* field to return a list of all Users on the system.
   - Leave the *Search Users* field empty to return a list of all Users on the system.

   Do not click anywhere in the page until the page completely refreshes.
5. Browse or sort the list of users to locate the one you want to manage.
6. Click the *User Name* link to view or set policies and manage its iFolders.

Locating the Users in the Search Results

Scroll up and down to browse the search results and locate the user you want to manage. The combination of the username, first name, and last name should help you locate the user.

- **Type:** Shows the member type of the user currently logged in. If the user is an individual user the interface also display an option for User Groups. If the user is a member of an Ldap Group, the interface lists all the members of the Ldap Group under the option for Group Members. An icon indicate whether the user has the iFolder Admin right (user wearing a referee-striped uniform) or is a normal user (user icon).
- **User Name:** The username assigned to the user account, such as `jsmith`.
- **Full Name:** The first and last name of the user account.
- **LDAP Context:** The LDAP tree context is used for provisioning users in to iFolder.
- **Last Login Time** The time when the user last logged in to the iFolder system.
- **User Groups (applicable only for individual users):** Lists all the groups that the selected user belongs to.
- **Group Members (applicable only for LDAPGroups):** Lists all the members who belong to the selected LDAP Group.

Click the user's name to manage User policies and iFolders for the user.

12.3 Accessing And Viewing General User Account Information

The Web Admin console opens to the User Page which displays the user's type (Admin user or user), username, user's full name (if available), the server to which the user is provisioned and the user status (Enabled or Disabled).

Follow the steps given below to access the Users Details Page:

1. On the iFolder user page, use the search functionality to locate the user whose iFolder account you want to manage.
2. Click the user's name link to open the User Details page to the Users tab.

The User Details page will display the following user details for the selected user's iFolder account.

Table 12-1 *User Details*

Parameter	Description
User Name	The username assigned to the user account, such as jsmith or john.smith@example.com.
Full Name	The first and last name of the user account.
LDAP Context	The LDAP tree context is used for provisioning users in to iFolder.
Last Login Time	The last time the user logging in to the iFolder system.
User Groups (applicable only for individual users)	Lists all the groups that the selected user belongs to.

Parameter	Description
Group Members (applicable only for LDAPGroups)	Lists all the members who belong to the selected LDAP Group.

The User Details page displays the iFolders owned or shared by the user. Click the *All tab* to list all the iFolders both owned and shared. To view the iFolder owned by the user, click the *Owned* tab. The *Shared* tab lists all the shared iFolders for this particular user account.

12.3.1 Enabling or Disabling an iFolder For an User Account

Follow the steps given below to enable or disable an iFolder for a given user account:

1. Locate the iFolder you want to manage, then select the check box next to the iFolder.
2. Click Enable to enable the iFolder.

   This allows the user to log in and synchronize iFolders.
3. Click Disable to disable the iFolder.
4. If the user is logged in when you make this change, the user's session continues until the user logs out. The policy takes effect the next time the user attempts to log in to the account. To have the lockout take effect immediately, you must restart the Apache services for the iFolder server, which disconnects all active sessions, including the user's session.

12.3.2 Deleting An iFolder

To delete an iFolder:

1. Locate the iFolder you want to delete, then select the check box next to the iFolder.
2. Click *Delete*.

12.4 Configuring User Account Policies

- Section 12.4.1, "Viewing the Current User Account Policies," on page 172
- Section 12.4.2, "Modifying User Account Policies," on page 174

12.4.1 Viewing the Current User Account Policies

1. In Web Admin console, select *Users* tab to view a list of current iFolder users.
2. Click the link for the user's name to open the User page for that user account.
3. You can view the following information below Policies:

Parameter	Description
Account	Specifies whether the user is currently allowed to log in to synchronize iFolders. You can select the check box to disable the User login.

Parameter	Description
No of iFolder per users	Specifies the maximum number of iFolder that a user can own. After Applying this policy, the user is limited to own a certain number of iFolders.The user who exceeds his or her usage limit receives an error message about the policy violation. If the limit is zero, the user cannot create any iFolders.
Disk Quota	**Limit:** Specifies the maximum space allotted on the server for this selected user. **Used:** Specifies the total space currently in use on the server for all iFolders owned by this selected user. **Available:** Specifies the difference between any space restrictions on the account and the space currently in use. If no quota is in effect, the value is No Limit. **Effective:** Effective space allocated on the server.
File size	Specifies the maximum total space (in MB) that a user's iFolder file is allowed to use, across all iFolders the user owns. A user quota supersedes a system-wide quota, whether the user quota is larger or smaller than the system-wide quota. The user quota can then be limited, but not increased by a policy on an iFolder. **IMPORTANT:** Users cannot successfully synchronize files of a size that would cause a quota to be exceeded. If they try to do so, only part of the file is synchronized, resulting in data corruption. If the total space consumed by iFolder file is nearing an effective quota (system, user, or iFolder), the user should stop synchronizing files until one or more of the following tasks results in enough space to safely synchronize the user's files in the iFolder where the file resides: ◆ The system-wide quota, user quota for the iFolder owner, and the iFolder quota are modified as needed. ◆ Files are moved from any of the iFolders owned by the user to another location where they no longer affect the effective quota, or files are deleted to clear space. ◆ Files are moved from the iFolder to another location where they no longer affect the effective quota, or its files are deleted to clear space.
Excluded files	Specifies to allow all file types or lists the file types to exclude from synchronization for the selected user's account. The file manager files called `thumbs.db` and `.DS_Store` are never synchronized. You do not need to keep these files, and synchronizing them results in repeated file conflict errors. If you have not set any individual restrictions for this user, this field reports `thumbs.db` and `.DS_Store` as part of the system-wide file-type restrictions. After you set individual file-type restrictions for the user, the user's settings are displayed instead. Even if the `thumbs.db` and `.DS_Store` restrictions are not displayed, they always apply; you cannot override them.

Parameter	Description
Synchronization	Specifies the minimum interval (in minutes) that a user's client can check iFolder data on the server and iFolder data on local iFolders to identify files that need to be downloaded or uploaded. Longer interval limits are more restrictive than shorter ones. **Interval:** If a user policy is set, it overrides the system policy, whether the user's interval is shorter or longer in value. **Effective:** Specifies the current synchronization interval. For example, if the user sets a synchronization interval that is less than (more frequent) than the system minimum, the system setting applies. The effective minimum synchronization interval is always the largest value from the following settings: ◆ The system policy (default of zero (`0`)), unless there is a user policy set. If a user policy is set, the user policy overrides the system policy, whether the user policy is larger or smaller in value. ◆ The local machine policy, or the setting on the client machine synchronizing with the server. ◆ The iFolder (collection) policy.
Encryption	Specifies the encryption policy for the selected iFolder user.
Sharing	Specifies the sharing policy for the selected iFolder user.

12.4.2 Modifying User Account Policies

1. In Web Admin console click the user name link listed under User's tab to open the user page
2. On the User page opened for that user account, you can select or deselect the following:

Parameter	Description
Account	Select the *Disable User Login* check box to disable the account for login. Deselect the value to enable the account for login. If the user is logged in when you make this change, the user's session continues until the user logs out. The policy takes effect the next time the user attempts to log in to the account. To have the lockout take effect immediately, you must restart the Apache services for the iFolder server, which disconnects all active sessions, including the user's session. Default Value: Enabled, Yes

Parameter	Description
No of iFolder per users	Specifies the maximum number of iFolder that a user can own. After Applying this policy, the user is limited to own a certain number of iFolders.The user who exceeds his or her usage limit receives an error message about the policy violation. If the limit is zero, the user cannot create any iFolders. Select *Limit* to enable the iFolder per users limit, and specify the number in the field. The policy setting does not affect the number of iFolders that the user already owns. If the number of iFolders owned by the user already exceeds the limit that you set, he or she can still own those iFolders. User level policy overrides LDAPGroup level and system level policy. Default Value: Disabled, no value set
Disk Quota	Specifies the maximum space allotted on the server for this selected user. Deselect *Limit* if there is no individual user quota, or to accept the system-wide quota for the selected user account. Select *Limit* to enforce a user quota, then specify the total space quota (in MB) for the selected user account.
File size	Specifies the maximum total space (in MB) that a user's iFolder data is allowed to use, across all iFolders the user owns for the selected user account. Deselect *Limit* if there is no individual user quota, or to accept the system-wide quota for the selected user account. Select *Limit* to enforce a user quota, then specify the total space quota (in MB) for the selected user account. If you enable a user space limit that is less than a user's current total space for iFolder data, the user's data stops synchronizing until the data is decreased below the limit or until the quota is increased to a value that is larger than the user's total space consumed. Default Value: Disabled or the system-wide quota if it is set.
Excluded Files	You can restrict some file types for this user, then specify the exclusion filters that determine the file types that can be synchronized for the user account. To add a file extension to exclusion filter, type the extension (such as `*.mpg`), then click *Add* to apply the filter. To exclude a file type from the restricted file types, select the check box adjacent to the file type, then click *Allow*. Default Value: The System-wide settings.
Synchronization	Select the check box to enable a minimum synchronization interval, then specify the minimum interval (in minutes). For example, a practical value is 600 seconds (10 minutes). Deselect the check box to set no synchronization interval or to accept the system-wide setting for the user account. If no value is set for system-wide or user policies, the value reported is `No Limit`. Default Value: Disabled, System-wide policy.

Parameter	Description
Encryption	You have two options for encryption to select from: *On* and *Enforced* **On:** Select *On* to enable Encryption. With this, user is allowed to set encryption policy for his or her iFolder files. User will have the control over the sharing of his iFolder data. **Enforced:** Select *Enforced* to enable encryption policy for the iFolder files of the selected user account. **IMPORTANT:** This option is enabled only if the system level encryption policy is set to *On*.
Sharing	You have three options for *Sharing* to select from: *On*, *Enforced* and *Revoke*. **On:** By default, iFolder sharing is enabled. Select *On* to disable sharing for the selected user. After applying this policy, user is not allowed to share his or her iFolders with others. However, you can still change the policy settings at iFolder level. **Enforce:** Select *Enforce* to enforce the policy set for the selected user. After applying this policy, the user cannot share his or her iFolders with others. **Revoke:** Select *Revoke* to remove the shared members of all the iFolders that belong to the selected user.

12.5 Enabling and Disabling iFolder User Accounts

Disabling a user's account temporarily, as opposed to deleting the user account, turns off the ability of that user to log in to the iFolder server. The user remains a valid iFolder user, can be shared with, and his or her iFolders are not orphans. The user cannot log in and, therefore, cannot synchronize (up or down) any data until the account is again enabled.

1. In Web Admin console, select *Users* tab.
2. Search for the user whose account you want to enable or disable for login.
3. Do one of the following:
   - Enable login for the user account by selecting *Enable*.
   - Disable login for the user account by selecting *Disable*.

13 Managing iFolders

This section discusses how to use the Novell iFolder Web Admin console to view details and configure iFolder policies.

- Section 13.1, “Accessing the iFolders Details Page,” on page 177
- Section 13.2, “Viewing The iFolder Details,” on page 177
- Section 13.3, “Searching for an iFolder,” on page 178
- Section 13.4, “Managing iFolder Members,” on page 179
- Section 13.5, “Managing an iFolder,” on page 179
- Section 13.6, “Managing iFolder Policies,” on page 181
- Section 13.7, “Enabling and Disabling an iFolder,” on page 183

13.1 Accessing the iFolders Details Page

1. Use the search functionality to locate the iFolder you want to manage.
2. Click the name of the iFolder to open the iFolder Details page.

   For more details on search, see “Locating the iFolders in the Search Results” on page 179.

   The iFolder Details page will display the iFolder details, a list of members who own or share the iFolders, and policy settings for this particular iFolder.

13.2 Viewing The iFolder Details

You can view the following information:

Parameter	Description
Type	Normal iFolder Encrypted iFolder Shared iFolder
Name	The name assigned to the iFolder.
Description	A short description about the iFolder. You can edit this information. Click *Save* to save the changes.

Parameter	Description
Owner	The username of the owner of the selected iFolder. For orphaned iFolders, the iFolder Admin user is made the owner until the iFolder can be reassigned or deleted. The iFolder owner has the Full Control right to the iFolder. The owner manages membership and access rights for users, and can remove the Full Control right for any member. With an enterprise server, the disk space used by the owner's iFolders counts against the owner's user account quotas on the enterprise server. Click the username link to view the details of the iFolder owner.
Path	The actual location of the iFolder and its data on the server. For example: **/var/opt/novell/ifolder3/simias/SimiasFiles/e84fdc6e-3d51-49df-ae3f-8c9213c76994/<iFolder_Name>** In this example, **e84fdc6e-3d51-49df-ae3f-8c9213c76994** is the unique ID of the iFolder share.
Modified	The last modified time and date of the iFolder.
Directories	Total number of directories in the iFolder.
Files	Total number of files in the iFolder.
Orphan	Shows the selected iFolder is orphaned or not. For orphaned iFolders, the iFolder Admin becomes the owner until the iFolder can be reassigned to a new owner or is deleted.

13.3 Searching for an iFolder

1. Use one of the following methods to get a list of iFolders:
   - Click the *All* tab on the iFolders page.
   - Click the *Orphan* tab on the iFolders page to retrieve a list of orphaned iFolders.
2. Use one or more of the following search methods, then click Search:
   - Select *Equals* as the filter criterion, then type the name of the iFolder you want to locate in the Search iFolders field.
   - Select a filter criterion (*Begins With*, *Ends With*, *Contains, Equals*) for the name of the iFolder, then type one or more letters in the *Search iFolder*s field.
   - Type an asterisk (*) in the *Search iFolders* field to return a list of all iFolders on the system.
   - Leave the *Search* field empty to return a list of all iFolders on the system.

   Do not click anywhere in the page until the page completely refreshes, then you can browse or manage the iFolders listed in the Search Results report.
3. Browse the list of iFolders to locate the iFolder you want to manage.
4. Click the iFolder's name link to view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

Locating the iFolders in the Search Results

Scroll up and down to browse the search results and locate the iFolder you want to manage. The combination of the iFolder's name and owner help to identify the iFolder you seek.

13.4 Managing iFolder Members

You can view the members' name, type and access rights assigned to them. You are allowed to add or delete an owner, assign ownership, and set access rights to a selected member. For more information, see Section 13.5, "Managing an iFolder," on page 179.

13.5 Managing an iFolder

Use the *iFolder* tab to manage membership in an iFolder.

- Section 13.5.1, "Adding a Member," on page 179
- Section 13.5.2, "Understanding iFolder Access Rights," on page 179
- Section 13.5.3, "Setting the iFolder Access Right for a Member," on page 180
- Section 13.5.4, "Removing a Member," on page 180
- Section 13.5.5, "Transferring Ownership of an iFolder," on page 181
- Section 13.5.6, "Managing Orphaned iFolders," on page 181

For iFolder 3.2 and earlier versions, when an owner adds a user to an iFolder, the user does not become a member until he or she accepts the iFolder on at least one computer. After the user accepts the invitation and sets up the iFolder, the user shows up in the member list. Currently, if you add a user or an LDAP Group as a member of an iFolder from the Web Access console, then the user or each LDAP Group member automatically becomes a member. The user and the iFolder will show up in the Web access interface without the user setting up a local iFolder on his or her computer.

13.5.1 Adding a Member

1. On the iFolder Details page, click *Add*.
2. Search for the user you want to make a member, select the check box next to the user's name, then click *OK*.

   The user is given Read Only access to the iFolder.
3. (Optional) Select the check box next to the user, then specify the Access right as *Admin*, *Read Write*, or *Read Only* right.
4. Click *Set*.

   Wait for the page to refresh. The *Rights* column should reflect the new access right. A notification message inviting the user to participate is sent to the user's account.

13.5.2 Understanding iFolder Access Rights

For an overview of access rights, see Section 1.4.8, "iFolder Access Rights," on page 20.

NOTE: Members of an LDAP Group inherit the access rights set for that LDAP Group.

The following table describes the capabilities associated with each level of access for users.

Capabilities	Owner	Full Control	Read/ Write	Read Only
Transfer ownership of an iFolder to another iFolder user	Yes	No	No	No
Set a quota for the iFolder	Yes	No	No	No
Make the iFolder available to other users (sharing)	Yes	Yes	No	No
Make the iFolder unavailable to other users (stop sharing)	Yes	Yes, except the owner	No	No
Assign access rights for other users	Yes	Yes, except the owner	No	No
Read directories and files in the iFolder	Yes	Yes	Yes	Yes
Add, modify, or delete directories and files in the iFolder	Yes	Yes	Yes	No
Rename directories and files in an iFolder	Yes	Yes	Yes	Yes
Rename the iFolder	No	No	No	No
Set up an iFolder on multiple computers	Yes	Yes	Yes	Yes
Revert an iFolder (do not participate on a local computer)	Yes	Yes	Yes	Yes
Delete an available iFolder to decline participating	Yes	Yes	Yes	Yes
Delete the iFolder and delete the iFolder and its files from the server (make it a normal folder again and no longer share it with others)	Yes	No	No	No

13.5.3 Setting the iFolder Access Right for a Member

1. On the iFolder Details page, locate the iFolder user you want to manage.
2. Select the check box next to that iFolder user.
3. Select the Rights drop-down menu, then select the desired right (*Admin*, *Read/Writ*e, or *Read Only* right).

   Wait for the page to refresh. The user's icon should reflect the new access right.

13.5.4 Removing a Member

1. Locate the iFolder you want to manage, then click the iFolder's name link to open the iFolder Details page to the iFolder tab.
2. On the *iFolder Details* page, select the check box next to the member user's name.
3. Select the *Members* tab, then select the check box next to the member user's name.

4 Click *Delete*.

The user's local copy of the data remains on the user's computer, but the user no longer has access to the server copy of the iFolder data.

13.5.5 Transferring Ownership of an iFolder

When you change the owner of an iFolder, the existing owner becomes a member of the iFolder and is assigned the Read/Write right. For orphaned iFolders, the iFolder Admin user becomes the owner.

1 On the iFolder Details page, search for the user you want to assign as the new owner of the iFolder.

2 Select the check box next to the user's name, then click *Owner*.

13.5.6 Managing Orphaned iFolders

An iFolder becomes orphaned when its owner is no longer provisioned for iFolder services. Orphaned iFolders are automatically assigned to the iFolder Admin user, who serves as a temporary owner until the iFolder can be assigned or deleted. Meanwhile, the members of the iFolder can continue to use it under the policies and access controls that were in place at the time the iFolder became orphaned.

1 On the iFolder details page, click *Orphan* tab to open the list of orphaned iFolders.

2 Browse to locate the orphaned iFolder you want to manage.

3 Click the iFolder name link to open the iFolder Details page.

Under the title *iFolder details*, the iFolder details page display the property *Orphan:Yes*.

4 Click *Adopt* to select the owner for the Orphaned iFolder.

5 Select an owner for the owner from the list of iFolder members

When you click Adopt, the iFolder details page lists all the members of that domain. The default owner for the orphaned iFolder is the Admin, who can assign himself or herself as the owner of the iFolder.

The name of the orphaned owner also is listed, if he or she is present in the current domain, and you can be re-assigned the orphaned owner as the owner.

The ownership is removed from you (default owner) after a member is selected as the owner of the orphaned iFolder. The specified user becomes the iFolder's owner and has the Full Control right to the iFolder. The Admin user, then will have only read permissions on that iFolder.

The orphaned property is deleted for that iFolder and it becomes a normal iFolder.

13.6 Managing iFolder Policies

Use the iFolder Policy tab to view and manage the policies for an iFolder.

1 Select *iFolders* or *Orphaned iFolders*.

2 Locate the iFolder you want to manage, then click the iFolder's name link to open the iFolder management page to the General tab.

3 Click the *Policy* tab, then click *Modify*.

4 Configure one or more of the following values, then click *Save* to apply the new settings:

Parameter	Description
Disable Synchronization	Select this to disable the synchronization of data in the iFolder. Deselect this to turn on synchronization, usually temporarily. Default Value: Enabled, Yes
Disk Quota	Select the Limit check box, then specify the maximum size (in MB) for the selected iFolder. If you enable a system-wide iFolder quota, a user's account quota overrides it, whether the user quota is lower or higher than the system quota. Default Value: Disabled, 100MB
Used (View only)	Reports how much space the iFolder data currently consumes.
Available (View only)	Reports how much space is available on the server for the iFolder data.
Effective (View only)	Reports effective space available on the server for the iFolder data.
File Size	**Limit:** Specifies the maximum total file size (in MB) that an iFolder user is allowed to use, across all iFolders the user owns for the selected user account. **Effective:** Effective file size allocated for the user. **IMPORTANT:** Users cannot successfully synchronize files of a size that would cause a quota to be exceeded. If they try to do so, only part of the file is synchronized, resulting in data corruption.
Excluded Files	Specifies a list of file types to include or to exclude from synchronization for the selected iFolder. The file manager files called `thumbs.db` and `.DS_Store` are never synchronized. To add a file extension to an inclusion or exclusion filter, type the extension (such as *.mpg), then click *Add* to apply the filter. To exclude a file type from the restricted file types, select the check box adjacent to the file type, then click *Delete*. Default Value: Disabled, Allow all file types or the System-wide settings.

Parameter	Description
Synchronization	Select the *Synchronization Interval* check box to enable a minimum interval setting for the selected iFolder, then specify the minimum value in minutes that users are allowed to set on their clients. To disable the setting, deselect the *Synchronization Interval* check box. If the option is disabled, the value reported is `No Limit`. If this option is enabled, the minimum synchronization interval specifies the minimum interval in minutes that a user's client can check iFolder data on the server and local iFolders to identify files that need to be downloaded or uploaded. If the iFolder is locked by an active system process (such as backup), you receive an Already Locked Exception (`AlreadyLockedException`) error. You cannot enable or disable synchronization for the iFolder until that process ends; try again later. The effective minimum synchronization interval is always the largest value from the following settings: ◆ The system policy (default of 5 minutes), unless there is a user policy set. If a user policy is set, the user policy overrides the system policy, whether it is larger or smaller in value ◆ The local machine policy, or the setting on the client system synchronizing with the server ◆ The iFolder policy Default Value: 5 minutes. You can lower it to a minimum of 5 seconds.
Sharing	**On:** By default, iFolder sharing is enabled. Deselect *On* to disable sharing for the selected iFolder. After applying this policy, iFolder cannot be shared either by the Admin or by the Owner of the iFolder. **Revoke:** Select *Revoke* to remove all the members from the list of shared members for the selected iFolder. **IMPORTANT:** Both of these option are disabled if you enable the *Disable Sharing* option at System level, LDAP Group level or User level.

13.7 Enabling and Disabling an iFolder

1. Click iFolders tab to open iFolders page.
2. Locate the iFolder you want to manage, then select the check box next to the iFolder name.
3. Select an action to perform on the iFolder:
   - Click Enable to enable the iFolder.

     This allows the user to access the iFolder and synchronize the files in it. By default, all iFolders are enabled.
   - Click *Disable* to disable the iFolder.

     If the user is logged in when you make this change, the user's session continues until the user logs out. The policy takes effect the next time the user attempts to log in to the account. To have the lockout take effect immediately, you must restart the Apache services for the iFolder server, which disconnects all active sessions, including the user's session.

NOTE: Disabling synchronization temporarily, as opposed to deleting or disabling the entire user account, turns off the ability of the selected iFolder to synchronize.

14 Managing an iFolder Web Access Server

This section describes how to manage your iFolder Web Access server.

- Section 14.1, “Starting iFolder Web Access Services,” on page 185
- Section 14.2, “Stopping iFolder Web Access Services,” on page 185
- Section 14.3, “Distributing the Web Access Server URL to Users,” on page 185
- Section 14.4, “Configuring the HTTP Runtime Parameters,” on page 185
- Section 14.5, “Securing Web Access Server Communications,” on page 187

14.1 Starting iFolder Web Access Services

iFolder Web Access services start whenever you reboot the system or whenever you start Apache services.

As a root user, enter the following command at the terminal console:

```
/etc/init.d/apache2 start
```

14.2 Stopping iFolder Web Access Services

iFolder services stop whenever you stop the system or whenever you stop Apache services.

As a root user, enter the following command at the terminal console:

```
/etc/init.d/apache2 stop
```

14.3 Distributing the Web Access Server URL to Users

After you install and configure the iFolder Web Access server, distribute the URL of the server Login page to users.

14.4 Configuring the HTTP Runtime Parameters

Two HTTP runtime parameters—Execution Time-Out (`executionTimeout`) and Maximum Request Length (`maxRequestLength`)—can affect the successful upload of a file to the Web Access server. The following table defines these run time parameters and their default values:

Parameter	Description
`executionTimeout`	The interval of time in seconds to wait between the command to upload a file and the successful execution where the file is stored on the iFolder enterprise server. Default Value: 720 (in seconds)

Parameter	Description
maxRequestLength	The maximum file size in bytes that a user is allowed to upload to the server via the Web Access server. The default maximum size is 1 GB for Web access. Default Value: 1048576 (in KB)

Using Web Access, a user can upload a local file to the user's iFolder on the enterprise server. If the file does not upload successfully before the interval times out or if the file size exceeds the allowed maximum, the upload is stopped and reported as a failure. Because the Web browser is controlling the errors, a problem of timing out or exceeding the maximum size might result in a Bad Request or other generic error.

The Execution Time-Out and Maximum Request Length parameters must be configured with compatible settings in the `/usr/lib/simias/web/web.config file` for the iFolder enterprise server and in the `/opt/novell/ifolder3/lib/simias/webaccess/Web.config` file for the Web Access server. The settings in `Web.config` for the enterprise server must be the same size or larger than the settings in `../webaccess/Web.config` for the Web Access server.

For example, the following code is the httpRuntime element with the default settings in the `../webaccess/Web.config` file for Web Access:

```
<httpRuntime
     executionTimeout="720"
     maxRequestLength="1048576"
/>
```

To modify the httpRuntime parameters:

1. Stop iFolder.
2. Set the httpRuntime parameters on the iFolder Web Access server by editing the values in the `/opt/novell/ifolder3/lib/simias/webaccess/Web.config` file.
3. If necessary, set the httpRuntime parameters on the iFolder enterprise server by editing the values in the `/usr/lib/simias/web/web.config` file.
4. Start iFolder.

For example, to set the time-out to 5 minutes (300 seconds) and the maximum file size to 5 megabytes (5120 KB) for the Web Access server, modify its httpRuntime parameter values in the `../webaccess/Web.config` file:

```
<httpRuntime
     executionTimeout="720"
     maxRequestLength="1048576"
/>
```

If the `webaccess/Web.config` values exceed the values in `web/web.config` for the enterprise server, you must also increase the sizes of runtime parameters in that file.

14.5 Securing Web Access Server Communications

This section describes how to configure SSL traffic between the iFolder Web Access server and other components. HTTPS (SSL) encrypts information transmitted over shared IP networks and the Internet. It helps protect your sensitive information from data interception or tampering.

- Section 14.5.1, “Using SSL for Secure Communications,” on page 187
- Section 14.5.2, “Configuring the SSL Cipher Suites and Protocol for the Apache Server,” on page 187
- Section 14.5.3, “Configuring the Web Access Server for SSL Communications with the Enterprise Server,” on page 188
- Section 14.5.4, “Configuring the Web Access Server for SSL Communications with Web Browsers,” on page 189
- Section 14.5.5, “Configuring an SSL Certificate for the Web Access Server,” on page 189

For information on how to configure SSL traffic on the iFolder enterprise server, see Section 10.12, “Securing Enterprise Server Communications,” on page 143.

14.5.1 Using SSL for Secure Communications

In a default deployment, Web Access server for iFolder uses SSL 3.0 for secure communications between components as shown in the following table.

iFolder Component	Enterprise Server	LDAP Server	Client	Web Browser
Web Access Server	Yes	Yes	No	Yes

For more information about SSL 3.0, see Section 10.12.1, “Using SSL for Secure Communications,” on page 143.

14.5.2 Configuring the SSL Cipher Suites and Protocol for the Apache Server

To ensure strong encryption, we strongly recommend the following configuration for the Apache server’s SSL cipher suite and protocol settings.

- Use only High and Medium security cipher suites, such as RC4 and RSA.
- Remove from consideration any ciphers that do not authenticate, such as Anonymous Diffie-Hellman (ADH) ciphers.
- Use TLS v1 and higher versions and disable SSL 2.0.
- Disable the Low, Export, and Null cipher suites.

To set these parameters, modify the aliases in the OpenSSL ciphers command (the SSLCipherSuite directive) in the `/etc/apache2/vhosts.d/vhost-ssl.conf` file.

1. Stop the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 stop
   ```

2 Open the `/etc/apache2/vhosts.d/vhost-ssl.conf` file in a text editor and do the following:

   2a Locate the SSLCipherSuite directive in the Virtual Hosts section and modify the plus (`+`) to a minus (`-`) in front of the ciphers you want to disable and make sure there is a `!` (not) before ADH:

   ```
   SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP:-eNULL
   ```

   2b Locate the SSLProtocol directive in the virtual hosts section and modify it include TLS v1:

   ```
   SSL Protocol TLSv1
   ```

3 Save your changes.

4 Start the Apache server: At a terminal console, enter

```
/etc/init.d/apache2 start
```

For more information about configuring strong SSL/TLS security solutions, see SSL/TLS Strong Encryption: How-To (http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html) on the Apache.org Web site.

14.5.3 Configuring the Web Access Server for SSL Communications with the Enterprise Server

The setting is stored in the `/opt/novell/ifolder3/lib/simias/webaccess/Web.config` file under the following tag:

```
<add   key="SimiasUrl" value="https://localhost"   />
<add key="SimiasCert" value=<raw certificate data in base 64 encoding>   />
```

If you disable SSL between Web Access server and the enterprise server and if the two servers are on different machines, you must also disable the iFolder server SSL requirement. Because the enterprise SSL setting also controls the traffic between the enterprise server and the client, all Web traffic between servers and between the clients and the enterprise server would be insecure.

IMPORTANT: Do not disable SSL on the Web Access server if the two servers are on different machines.

If the two servers are running on the same machine and you want to disable SSL, rerun the configuration, and specify `http://localhost` as the URL for the enterprise server. By default, the Web Browser is configured to communicate with the iFolder Web Access server and the iFolder Enterprise server via SSL. iFolder uses HTTP BASIC for authentication, which means passwords are sent to the server in the clear. If the iFolder deployment is in large scale and the Web Access server is on a different machine than the iFolder enterprise server, an Administrator could reconfigure to enable SSL between the Web Access Server and the iFolder Enterprise Server, which would increase the security for communications between the two servers. This is a recommended setting

14.5.4 Configuring the Web Access Server for SSL Communications with Web Browsers

The iFolder 3.*x* Web Access server requires a secure connection between the user's Web browser and the Web Access server. The SSL connection supports the secure exchange of data. For most deployments, this setting should not be changed because iFolder uses HTTP BASIC for authentication, which means passwords are sent to the server in the clear. Without SSL encryption, the iFolder data is also sent in the clear.

The following Rewrite parameters control this behavior and are located in the `/etc/apache2/conf.d/ifolder_web.conf` file:

```
LoadModule rewrite_module /usr/lib/apache2/mod_rewrite.so

RewriteEngine On

RewriteCond %{HTTPS} !=on

RewriteRule ^/ifolder/(.*) https://%{SERVER_NAME}/ifolder/$1 [R,L]
```

To disable the requirement for SSL connections, you can comment out these Rewrite command lines in the `ifolder_web.conf` file. Placing a pound sign (`#`) at the beginning of each line renders it as a comment.

WARNING: Without an SSL connection, traffic between a user's Web browser and the Web Access server is not secure.

To disable the SSL requirement:

1. Stop the iFolder Web Access services.
2. Edit the `/etc/apache2/conf.d/ifolder_web.conf` file to comment out the Rewrite command lines.

   For example:

   ```
   #LoadModule rewrite_module /usr/lib/apache2/mod_rewrite.so

   #RewriteEngine On

   #RewriteCond %{HTTPS} !=on

   #RewriteRule ^/ifolder/(.*) https://%{SERVER_NAME}/ifolder/$1 [R,L]
   ```
3. Start the iFolder Web Access services.

14.5.5 Configuring an SSL Certificate for the Web Access Server

For information, see "Managing SSL Certificates for Apache" on page 221.

15 Troubleshooting Tips For Novell iFolder

This section gives you a list of troubleshooting suggestions that can help you resolve some of the iFolder issues.

- Section 15.1, “On Upgrading the Server from OES 2 SP3 to OES 11, iFolder Fails to Function,” on page 192
- Section 15.2, “iFolder Client on MAC Fails to Reconnect to the iFolder Server after Sleep,” on page 193
- Section 15.3, “iFolder Slave Server Fails to Configure and Reports a 401 Unauthorized Error,” on page 193
- Section 15.4, “iFolder Post Install on an Upgraded Server Might Result in Failure to Access iFolder Server,” on page 193
- Section 15.5, “iFolder Server Configuration Fails on Upgrading to OES 11 SP1 server,” on page 193
- Section 15.6, “Uploading of Files is Possible Only if the Secondary Administrator Sets the Disk Quota,” on page 193
- Section 15.7, “Reprovisioning Users From One Server to Another Results in Creation of Duplicate Entries of iFolders for the Reprovisioned User,” on page 194
- Section 15.8, “iFolder Does Not Support Spaces or Dots in the Admin DN and User Container DN,” on page 194
- Section 15.9, “iFolder Deletion Leaves an Empty Directory on the Server,” on page 194
- Section 15.10, “No Auto Upgrade For the iFolder Mac Client,” on page 194
- Section 15.11, “Menus for the iFolder Client on Mac are Inconsistent with Menus on Windows and Linux,” on page 194
- Section 15.12, “Unable to Create a New Account After Deletion of a Previous Account,” on page 195
- Section 15.13, “The iFolder Icon Is Not Updated Automatically on SLES and SLED 11,” on page 195
- Section 15.14, “Delta Sync Is Not Supported for Encrypted iFolders,” on page 195
- Section 15.15, “The namcd Services Must Be Running While Changing the Proxy User Password by Using Common Proxy Script,” on page 195
- Section 15.16, “The iFolder Web Admin Alias Name Does Not Support Spaces,” on page 195
- Section 15.17, “iFolder Configuration Fails at Random,” on page 195
- Section 15.18, “Setting Up the NSS file System Trustee Rights,” on page 196
- Section 15.19, “Login to Web Admin and Web Access Console Fails with an Error Message,” on page 196
- Section 15.20, “iFolder Full Restore Using nbackup fails to restore in a Cluster Environment,” on page 196
- Section 15.21, “Exception Error When Datapath on Server is not Mounted,” on page 196
- Section 15.22, “Temporary files are getting synchronized as actual files,” on page 197
- Section 15.23, “Web Admin Console Fails to Start Up,” on page 197

- Section 15.24, “Login to the Web Console Fails,” on page 197
- Section 15.25, “The OES Common Proxy User Password is Not Always Compliant with the Password Policies,” on page 198
- Section 15.26, “Enabling a Large Number of Users at the Same Time Times Out,” on page 198
- Section 15.27, “Changes Are Not Reflected After Identity Sync Interval,” on page 198
- Section 15.28, “Synchronizing a Large Number of Files Randomly Requires Multiple Sync Cycles,” on page 198
- Section 15.29, “iFolder Data Does Not Sync and Cannot be Removed from the Server,” on page 198
- Section 15.30, “Samba Connection to the Remote Windows Host Times out,” on page 199
- Section 15.31, “Exception Error while Configuring iFolder on a Samba Volume,” on page 199
- Section 15.32, “LDAP Users Are Not Reflected in iFolder,” on page 199
- Section 15.33, “Directory Access Exception on Creating or Synchronizing iFolders,” on page 199
- Section 15.34, “Changing Permission to the Full Path Fails,” on page 199
- Section 15.35, “List of Items Fails to Synchronize,” on page 199
- Section 15.36, “Access Permission Error While Logging in Through Web Access,” on page 200
- Section 15.37, “Web Admin and Web Access Show a Blank Page,” on page 200
- Section 15.38, “Option to Start iFolder During System Login Does Not Work in the iFolder Client for SLED 11,” on page 200
- Section 15.39, “On running simias-server-setup, the setup fails while configuring SSL,” on page 200
- Section 15.40, “iFolder linux client fails to startup if the datapath does not have any contents,” on page 201
- Section 15.41, “Incremental Patch Upgrade Issue in a Multiple-Server Scenario,” on page 201

15.1 On Upgrading the Server from OES 2 SP3 to OES 11, iFolder Fails to Function

On upgrading the server to OES 11, the mono key store breaks, hence iFolder fails to function.

To resolve this issue, on upgrading to OES 11, perform the following steps:

1. To remove the mono certificate, run

   ```
   certmgr -del -c -m Trust 1B00FEDEEEFAE2B447D1769F289590E4434208AC
   ```

2. To re-import the mono certificate, run

   ```
   -add -c -m Trust /tmp/acuityca.crt
   ```

3. To reconfigure the iFolder server using YaST, run

   ```
   yast2 novell-ifolder3
   ```

   3a In the Novell iFolder System Configuration Options screen, do the following:

   - Deselect *iFolder Server*
   - Select *iFolder Web Admin*
   - Select *iFolder Web Access*

4. Restart Apache.

15.2 iFolder Client on MAC Fails to Reconnect to the iFolder Server after Sleep

To resolve this issue on the MAC iFolder client, modify the following TCP parameters in the sysctl.conf file:

```
net.inet.tcp.delayed_ack=0
net.inet.tcp.mssdflt=1440
kern.ipc.maxsockbuf=500000
net.inet.tcp.sendspace=250000
net.inet.tcp.recvspace=250000
```

15.3 iFolder Slave Server Fails to Configure and Reports a 401 Unauthorized Error

While configuring iFolder slave server, the configuration fails with a 401 unauthorized error. If you receive this error, you must verify that the LDAP admin user has supervisory and attribute rights on the LDAP search context(s) specified during the configuration.

NOTE: It is recommended to use only service-specific proxy user for iFolder proxy and not any other user accounts.

15.4 iFolder Post Install on an Upgraded Server Might Result in Failure to Access iFolder Server

If you upgrade an OES server and then post install iFolder users may not be able to access iFolder services. This is because during iFolder configuration, necessary rights are not available to the user wwwrun on `/var/lib/wwwrun/` directory. You must manually assign read,write, and execute rights to wwwrun on `/var/lib/wwwrun/` directory.

15.5 iFolder Server Configuration Fails on Upgrading to OES 11 SP1 server

The failure of iFolder configuration is caused randomly when authentication to Mono fails. Reconfiguring iFolder resolves this issue.

15.6 Uploading of Files is Possible Only if the Secondary Administrator Sets the Disk Quota

After you create a secondary administrator and assign a group to the secondary administrator, the secondary administrator must assign a disk quota to the users of the group. Otherwise, the users cannot upload any files by using the Web Access console or the iFolder client. This is applicable only if the Administrator console option was selected for managing the group quota while creating the secondary administrator. However, users can create empty iFolders even if the secondary administrator has not set any disk quota for users.

15.7 Reprovisioning Users From One Server to Another Results in Creation of Duplicate Entries of iFolders for the Reprovisioned User

If you reprovision users from one server to another, duplicate entries of iFolders are sometimes displayed for the reprovisioned user in the Web console and iFolder clients.

As a workaround, after you reprovision the users, you must log in to the Web Admin console to verify if duplicate entries of iFolders are displayed for reprovisioned users. If duplicate entries are displayed, you must restart the iFolder server to resolve the issue.

15.8 iFolder Does Not Support Spaces or Dots in the Admin DN and User Container DN

iFolder does not support spaces or dots in the admin DN and user container DN. If the Admin DN or user container DN has a space or dot in it, iFolder configuration fails. This is applicable for all directory services.

15.9 iFolder Deletion Leaves an Empty Directory on the Server

For every iFolder, a directory with iFolder's unique ID as its name is created on the server. All the iFolder data is stored in this directory. When you delete an iFolder, the content of the directory is deleted. However, the directory itself is not deleted.

15.10 No Auto Upgrade For the iFolder Mac Client

The iFolder client for Macintosh doesn’t provide the auto upgrade feature. When a new version of the client is available, iFolder prompts you about the availability of the client for downloading, and when you click *OK*, it downloads the client to a location on your workstation. You need to go to that location and manually install the new client.

15.11 Menus for the iFolder Client on Mac are Inconsistent with Menus on Windows and Linux

There is an inconsistency in menus for clients on Mac in comparison to the clients on Windows and Linux. For instance, for the iFolder client in Mac, both *Delete* and *Revert to Normal iFolder* options are enabled for both local and remote iFolders.

15.12 Unable to Create a New Account After Deletion of a Previous Account

If you delete a previously configured account and create any new account by using the account creation wizard, you might receive an error. This is a rare occurrence.

If you receive this error, you must stop the iFolder client, delete the local simias directory (`$HOME/.local/share/simias)`, then create a new account.

15.13 The iFolder Icon Is Not Updated Automatically on SLES and SLED 11

For iFolder clients on SLES and SLED 11, if you convert a folder to an iFolder or revert an iFolder to a regular folder, the icon on iFolder is not updated automatically.

As a workaround for this issue, you must do a manual refresh. For instance, you can manually refresh by pressing the F5 key.

15.14 Delta Sync Is Not Supported for Encrypted iFolders

Modifying any file in an encrypted iFolder performs a full sync to the iFolder server, instead of synchronizing only the changes.

15.15 The namcd Services Must Be Running While Changing the Proxy User Password by Using Common Proxy Script

If namcd services are down, you cannot change the common proxy user password by using common proxy script. This is because the Apache wwwrun user cannot be retrieved from the eDirectory if the namcd services are down.

15.16 The iFolder Web Admin Alias Name Does Not Support Spaces

You must ensure that the Web Admin alias name specified during iFolder configuration has no space. Otherwise, the Apache restart after iFolder configuration fails.

15.17 iFolder Configuration Fails at Random

During the OES2 SP3 server installation, the iFolder server configuration might fail. This is a rare occurrence. If this issue occurs, run `yast2 novell-ifolder3` to reconfigure the iFolder server.

15.18 Setting Up the NSS file System Trustee Rights

If you are using an NSS volume to store user data, you must set up the NSS file system trustee rights for the wwwrun Web server user object before restarting your Web server .

Open a terminal console on the server, log in as the root user or equivalent, then enter the following command:

```
rights -f /media/nss/NSSVOL -r rwfcem trustee wwwrun.ou.o.treename
```

If the file system trustee rights are not set up properly, you receive the following error message:

```
An Internal Error has occurred.
```

15.19 Login to Web Admin and Web Access Console Fails with an Error Message

During iFolder installation, if the certificate that you import to the iFolder server certificate store expires or if you change the certificate for the LDAP server, you will receive the following error when you attempt to login to the Web admin or Web access console:

```
Failed to authenticate, problem with Ldap or iFolder server certificate.
```

Consequently, iFolder will log appropriate error messages in the simias debug log. To successfully login again to the web admin or web access console, you must import the new certificate. To do this, run the `ldap-cert-update tool` from the `<iFolder install path>/bin location`.

This tool automatically detects the iFolder data path and the LDAP URL to fetch new certificates from. The tool displays the new certificate (if it is already changed on server) and enables you to import the same.

15.20 iFolder Full Restore Using nbackup fails to restore in a Cluster Environment

If the restoration fails and iFolder service does not come up, you must do the following:

1. Reconfigure the iFolder server using `yast2 novell-ifolder3` using the same values as done for the first time configuration.
2. Access the iFolder so that database gets initialized.
3. Restore the iFolder data by running the `nbackup` command again.

15.21 Exception Error When Datapath on Server is not Mounted

If datapath on server is not mounted, then iFolder server may fail to start and log the following message: `System.IO.DirectoryNotFoundException: Directory '/media/nss/IFVOL/DATA/simias' not found`.

As a workaround, you must verify the path and ensure that the nss volume is mounted and then restart Apache to start the iFolder server.

15.22 Temporary files are getting synchronized as actual files

Many applications such as MS Office generate some temporary files while editing a file. These files also get synchronized as actual files by iFolder. To avoid synchronization of such temporary files, you must modify the system policies of the iFolder server to exclude the temporary files from synchronization. To do this, follow the steps given below:

1. In the Web Admin console, click the *Systems* tab.
2. Specify the type of temporary files that you want to exclude in the *Excluded files* field and then click *Add*. For instance, to exclude temporary files with the extension `.tmp`, you must specify `*.tmp` in the *Excluded files* field.
3. Click *Save* to save the policy setting.

Filters can also be set at user level to exclude temporary files. To do this, in the *Users* tab of the Web Admin console, select a user and then add the temporary files to the excluded file list.

15.23 Web Admin Console Fails to Start Up

If the iFolder Web Admin console does not start on your first attempt:

1. Open a terminal console.
2. Run `/etc/init.d/apache2 stop` to stop the Apache process.
3. Run `ps -ef|grep mono` to check if any Mono process for iFolder is still running on the server side.
4. Run `kill <process id of the process>` to end the Mono process for iFolder.
5. Restart Apache.

15.24 Login to the Web Console Fails

If you cannot log in to Web Admin or Web Access console, consider the following causes:

15.24.1 Login Fails Randomly

To resolve the issue, do the following:

1. Open a terminal console.
2. Stop the Mono process
3. Restart the Apache process

15.24.2 A DSfW Server is Used as the LDAP Server.

The workaround for this issue is to ensure the following:

- iFolder Admin and iFolder proxy users are created on the DSfW server.
- iFolder is configured by using command line script `simias-server-setup`.
- Use port 1389 for non-SSL and port 1636 for SSL communications.

15.25 The OES Common Proxy User Password is Not Always Compliant with the Password Policies

If you have password policies that support non-ASCII passwords or that require passwords to be 4 characters or shorter, or 12 characters or longer, make sure you select the *Attach common proxy user to common proxy policy* option (the default setting) on the OES proxy install screen.

Selecting this option prevents the password-compliance issues with the proxy user after the installation.

If you are installing, then abort the installation and reinstall OES. In the common proxy page, you must provide a password for the common proxy user that complies with your password policy.

15.26 Enabling a Large Number of Users at the Same Time Times Out

In the Web Admin console, if enabling a large number of users at the same time throws a time-out error message, consider the following cause:

- The Web Admin console is opened by using Internet Explorer.

The workaround for this issue is to open the Web Admin console by using Mozilla Firefox.

15.27 Changes Are Not Reflected After Identity Sync Interval

The changes you have made in the iFolder domain, such as adding a new user to the iFolder domain from the LDAP, are not reflected even after the identity sync interval. The workaround is to click the *Sync Now* button after you make the changes.

15.28 Synchronizing a Large Number of Files Randomly Requires Multiple Sync Cycles

When you attempt to synchronize a large number of files, a few files are not synchronized in the first sync cycle. Complete synchronization of the files requires multiple sync cycles.

15.29 iFolder Data Does Not Sync and Cannot be Removed from the Server

In some cases, an iFolder fails to synchronize, and when you attempt to revert the iFolder to a normal folder, you get an exception error.

Although you can successfully revert that iFolder to a normal folder from other machines, the original client machine you used to upload the iFolder shows the same iFolder on the machine.

15.30 Samba Connection to the Remote Windows Host Times out

If Samba connection to the remote Windows host times out when you execute `samba mount` command, you must check whether the Windows firewall is enabled or not. If it is enabled, add the Samba port to the list of permitted ports in the firewall configuration.

15.31 Exception Error while Configuring iFolder on a Samba Volume

If iFolder server throws an exception when you configure iFolder server on a Samba volume, check the properties of the folder in Windows. You must provide the read-write permission to the network users. In other words, you must ensure that the *Read Only* check box is deselected

15.32 LDAP Users Are Not Reflected in iFolder

If the LDAP users are not synchronized immediately in iFolder, check to see if the default interval to synchronize the LDAP server with iFolder servers is 24 hours.

To reflect the changes immediately, you can use the *Sync now* option in the *Server details* page of the Web Admin console.

15.33 Directory Access Exception on Creating or Synchronizing iFolders

If the system throws Directory Access exception error when the user create or synchronize iFolder, check the owner and group of the directory in which the iFolder has been created. Ensure that you have set that to *wwwrun:www*.

15.34 Changing Permission to the Full Path Fails

If you cannot change the permission to the full path specified while configuring a multi-volume setup, use the following procedure:

1. Run `chown -R <apache user>:<apache group> <Data/store/path/simias>`.
2. Change the permission that has already been set.

15.35 List of Items Fails to Synchronize

If a list of items fails to synchronize, consider the following causes:

- You excluded the non-synchronized file types in the Web Admin console policy.
- The disk space restriction has been exceeded for the specified user or the specified iFolder.
- The user has the file or files open in an application. In this case, users must close the application and re-sync the iFolder.

15.36 Access Permission Error While Logging in Through Web Access

If the user cannot log in to iFolder Web Access, consider the following actions:

- Check the permission for the Apache user to the data store path of iFolder, and change permissions as necessary.
- Run `chown -R <apache user>:<apache group> <Data/store/path/simias>`.

15.37 Web Admin and Web Access Show a Blank Page

If the Web Admin console and Web Access console show blank pages, ensure that the Simias server and Web Access server are up and running.

15.38 Option to Start iFolder During System Login Does Not Work in the iFolder Client for SLED 11

For iFolder clients on SLED 11, if you leave iFolder running and log out of the system, iFolder does not start as expected during system reboot.

As a workaround, you must add iFolder to the list of startup programs:

1. Click the *Gnome Control Center*.
2. Click *Systems* > *Sessions*.
3. In the Sessions dialog box, click the *Startup Programs* tab.

   You can also open the Sessions dialog box from the command terminal by typing the command `gnome-session-properties`.
4. To add iFolder to the list of startup programs, click *Add* and browse to the location where the iFolder executable is available.

   IMPORTANT: The iFolder client executable is present in `/opt/novell/ifolder3/bin`.
5. Click *OK* and then click *Close* to close the Sessions dialog box.

15.39 On running simias-server-setup, the setup fails while configuring SSL

If you select the default options while running the `simias-server-setup` and if the setup fails while configuring SSL, you must ensure that Apache is SSL-enabled and configured to point to an SSL certificate on an iFolder server. For more information, see Section D.3, “Configuring Apache to Point to an SSL Certificate on an iFolder Server,” on page 222

15.40 iFolder linux client fails to startup if the datapath does not have any contents

For iFolder linux client, if the client datapath contains an empty simias folder, the ifolder client does not startup.

As a workaround to this issue, you must delete the empty simias folder from the location: `$HOME/.local/share/` and then restart the client.

15.41 Incremental Patch Upgrade Issue in a Multiple-Server Scenario

In a multiple-server scenario where all the iFolder servers are on OES 2 SP2 March 2010 or an earlier patch, if you upgrade any of these iFolder servers to a patch of OES 2 SP2 May 2010 or later, then the remaining iFolder servers cannot communicate with the upgraded iFolder servers.

In this scenario, for the iFolder servers to communicate with each other, the upgraded iFolder server must behave like the remaining iFolder servers until all the servers are upgraded to the same patch level (OES 2 SP2 May 2010 or later). To ensure that this happens, use the following procedure:

1. Create a backup of `the Simias.config` file located in the upgraded iFolder server datapath.
2. Add the following entry in the `Simias.config` file under server section:

   ```
   <setting name="MultiByteServer" value="no" />
   ```

3. Restart Apache.

After upgrading the remaining iFolder servers with the OES 2 SP2 May 2010 or later patch, you must edit the entry mentioned in Step 2, by changing the value of the attribute from no to yes, or delete the entry from the `Simias.config` file.

NOTE: The above issue does not occur for iFolder servers with OES 2 SP2 May 2010 and later patches.

---

16 Frequently Asked Questions

This section describes the frequently asked questions for managing iFolder:

- Section 16.1, “iFolder 3.9 Server,” on page 203
- Section 16.2, “iFolder Client,” on page 203
- Section 16.3, “iFolder Administration,” on page 204

For an additional listing of questions and answers that have been submitted by administrators and iFolder users, see the following:

- Chapter 15, “Troubleshooting Tips For Novell iFolder,” on page 191
- *Novell iFolder 3.9.2 Cross-Platform User Guide*
- iFolder 3 Web site (http://www.ifolder.com/index.php/)

16.1 iFolder 3.9 Server

This section addresses the following issues:

- Section 16.1.1, “Is iFolder server for 3.9 supported on a 64-bit OS?,” on page 203
- Section 16.1.2, “Is iFolder going to support non-eDirectory related platforms as an identity source?,” on page 203

16.1.1 Is iFolder server for 3.9 supported on a 64-bit OS?

Yes. Both the server and iFolder client for Linux work on 64-bit systems.

16.1.2 Is iFolder going to support non-eDirectory related platforms as an identity source?

Yes, it already does. Any open LDAP-based directory works seamlessly with iFolder 3.9.

16.2 iFolder Client

This section addresses the following issues:

- Section 16.2.1, “Is iFolder 3.9.2 version supported on the Macintosh platform?,” on page 204
- Section 16.2.2, “Can I use the iFolder 3.x client to connect to iFolder 3.9 server?,” on page 204
- Section 16.2.3, “Can I can use iFolder 3.9 version on different operating systems on different workstations to access and share the files?,” on page 204
- Section 16.2.4, “There was a 10 MB file limitation using Web Access? Is it still applicable for iFolder 3.9 version?,” on page 204
- Section 16.2.5, “I deleted a file accidentally. Can I recover it?,” on page 204

16.2.1 Is iFolder 3.9.2 version supported on the Macintosh platform?

iFolder 3.9.2 version supports Macintosh client 10.6 or later.

16.2.2 Can I use the iFolder 3.*x* client to connect to iFolder 3.9 server?

No. When you install iFolder 3.9 client, it overwrites the iFolder 3.*x* client if it is already installed and performs an in-place upgrade of the local store.

16.2.3 Can I can use iFolder 3.9 version on different operating systems on different workstations to access and share the files?

Yes. You can use iFolder for different operating systems on different workstations to access and share the files. For example, you can use an iFolder client on a Windows workstation at home and on a Linux workstation at the office to share the same files.

16.2.4 There was a 10 MB file limitation using Web Access? Is it still applicable for iFolder 3.9 version?

No. Web Access for iFolder 3.9 no longer has this file size limitation. For more information on the Web Access console, see "Using Web Access for Novell iFolder " in the *Novell iFolder 3.9.2 Cross-Platform User Guide*.

16.2.5 I deleted a file accidentally. Can I recover it?

Currently iFolder does not support this functionality.

16.3 iFolder Administration

This section addresses the following issues:

- Section 16.3.1, "What is the management console for iFolder 3.9?," on page 204
- Section 16.3.2, "What are the new features in the Web Admin console?," on page 205
- Section 16.3.3, "Can the administrator control the ability to encrypt iFolder files?," on page 205
- Section 16.3.4, "Are there any enhancements for how bulk users are enabled for iFolder?," on page 205
- Section 16.3.5, "How can the iFolder administrator manage the data owned by an iFolder user who has been removed from the iFolder domain?," on page 205

16.3.1 What is the management console for iFolder 3.9?

The management console for iFolder 3.9 is the Web Admin console. For more information on the Web Admin console, see Chapter 11, "Managing iFolder Services via Web Admin," on page 147.

16.3.2 What are the new features in the Web Admin console?

You can manage the multi-server and multi-volume features from the Web Admin console. You can generate reports at a granular level and export them to a text file for later viewing or offline management. You can manage policy settings for the iFolder system, users, and for iFolders. For more information on the Web Admin console, see Chapter 11, “Managing iFolder Services via Web Admin,” on page 147

16.3.3 Can the administrator control the ability to encrypt iFolder files?

Yes, the administrator can manage the encryption policy settings through the Web Admin console. For more information, see Section 11.4.4, “Configuring System Policies,” on page 156.

16.3.4 Are there any enhancements for how bulk users are enabled for iFolder?

iFolder users can be provisioned based on LDAP groups and containers. The users are provisioned during their first login. The client transparently redirects to the appropriate server in a Multi-server environment. For more information, see Section 3.5, “iFolder User Account Considerations,” on page 30.

16.3.5 How can the iFolder administrator manage the data owned by an iFolder user who has been removed from the iFolder domain?

If a user is deleted as a user for the iFolder system, the iFolders owned by the user are orphaned. Orphaned iFolders are assigned temporarily to the iFolder Admin user, who becomes the owner of the iFolder. These iFolders later can be assigned to other users by using the Web administration console. Membership and synchronization continue while the iFolder Admin user determines whether an orphaned iFolder should be deleted or assigned to a new owner. For more information, see Section 13.5.6, “Managing Orphaned iFolders,” on page 181.

A Caveats for Implementing iFolder Services

This section presents a few pointers for avoiding common implementation problems for iFolder.

The list that follows is not comprehensive. Rather, it simply outlines some of the more common problems reported by network administrators. To ensure successful service implementations, you should always follow the instructions in the documentation for the services you are implementing.

This section discusses the caveats to consider after installing and before implementing iFolder services.

- Section A.1, “iFolder User Move,” on page 207
- Section A.2, “Loading Certificates to the Recovery Agent Path,” on page 207
- Section A.3, “Using a Single Proxy User for a Multi-Server Setup,” on page 207
- Section A.4, “Slave Server Upgrade,” on page 208
- Section A.5, “Slave Configuration,” on page 208
- Section A.6, “Novell iFolder Admin User,” on page 208

A.1 iFolder User Move

- The user move must be initiated from the server it is provisioned to. For example, iFolder system has 2 servers OES 2 SP3 and OES 11 SP1. A user is provisioned to OES 2 SP3 server and needs to be moved to OES 11 SP1 server. Ensure to perform the user move task from the OES 2 SP3 server.
- In the Web access client, history functionality fails to work when a user is moved from the Master server to a Slave server.

A.2 Loading Certificates to the Recovery Agent Path

If the path to the key Recovery agent certificates is set during iFolder configuration, you must ensure that the certificates are copied to this location. The location is `datapath/simias/Simias.config` under the `RAPath` section.

For more information on the Recovery agent, refer to the Section 6.7, “Recovery Agent Certificates,” on page 87

A.3 Using a Single Proxy User for a Multi-Server Setup

By default, each server creates its own Proxy user for role separation. However, you can use single Proxy user for both master and slave servers. You can provide the Proxy DN and Proxy password for the master server configuration and for the slave configurations. You must not use the default configuration for the Proxy user.

A.4 Slave Server Upgrade

On updating the LDAP context on the Master server, ensure synchronization is successful before upgrading the Slave server.

A.5 Slave Configuration

Selecting *Install into existing Domain* during configuration is considered to be a slave configuration. If the option is not selected, the server you are configuring is considered to be a master.

A.6 Novell iFolder Admin User

By default, the LDAP admin assumes the iFolder Administrator position. You must change this default setting during the master server configuration to have a better role separation.

B Decommissioning a Slave Server

To remove a slave server that has users provisioned to it from an iFolder domain:

1. Reprovision all the users (including admin) on the slave server to a different server.
2. In the slave server, open a terminal prompt.
3. Enter `rcapache2 stop` to bring down the slave server.
4. Enter `/opt/novell/ifolder3/bin/simias-server-setup --remove` and follow the on-screen instructions.

C Configuration Files

- Section C.1, “Simias.config File,” on page 211
- Section C.2, “Web.config File for the Enterprise Server,” on page 212
- Section C.3, “Web.config File for the Web Admin Server,” on page 214
- Section C.4, “Web.config File for the Web Access Server,” on page 217

C.1 Simias.config File

The default locations of the `Simias.config` file is `<datapath>/simias/Simias.config`.

```
<configuration>
  <section name="EnterpriseDomain">
    <setting name="SystemName" value="iFolder" />
    <setting name="Description" value="iFolder Enterprise System" />
    <setting name="AdminName" value="cn=admin,o=novell" />
  </section>
  <section name="Server">
    <setting name="Name" value="npsdt-val-3" />
    <setting name="PublicAddress" value="https://192.168.1.1:443/simias10" />
    <setting name="PrivateAddress" value="https://192.168.1.1:443/simias10" />
    <setting name="RAPath" value="/var/simias/data/simias" />
  </section>
  <section name="Authentication">
    <setting name="SimiasAuthNotRequired" value="Registration.asmx, Login.ashx,
    Simias.asmx:PingSimias, DomainService.asmx:GetDomainID, pubrss.ashx,
    pubsfile.ashx, Simias.asmx:GetRAList, Simias.asmx:GetRACertificate" />
    <setting name="SimiasRequireSSL" value="no" />
  </section>
  <section name="Identity">
    <setting name="Assembly" value="Simias.LdapProvider" />
    <setting name="ServiceAssembly" value="Simias.Server" />
    <setting name="Class" value="Simias.LdapProvider.User" />
    <!--
      <setting name="Assembly" value="Simias.SimpleServer" />
      <setting name="Class" value="Simias.SimpleServer.User" />
      -->
```

```
    <!--
      <setting name="Assembly" value="Simias.MdbSync" />
      <setting name="Class" value="Simias.MdbSync.User" />
      -->
  </section>
  <section name="StoreProvider">
    <setting name="Assembly" value="SimiasLib.dll" />
    <setting name="Type" value="Simias.Storage.Provider.Flaim.FlaimProvider" />
    <setting name="Path" value="/var/simias/data/simias" />
  </section>
  <section name="LdapAuthentication">
    <setting name="LdapUri" value="ldaps://192.168.1.1/" />
    <setting name="ProxyDN" value="cn=iFolderProxy,o=novell" />
  </section>
  <section name="LdapProvider">
    <setting name="NamingAttribute" value="cn" />
    <setting name="Search">
      <Context dn="o=novell" />
    </setting>
  </section>
</configuration>
```

C.2 Web.config File for the Enterprise Server

By default, the `web.config` file for the enterprise server is in the `/usr/lib/simias/web/Web.config` directory. The following is an example of a configured file.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<!-- Enable this if you want gzip compression. Also uncomment the <mono.aspnet>
section below
  <configSections>
     <sectionGroup name="mono.aspnet">
     <section name="acceptEncoding"
        type="Mono.Http.Configuration.AcceptEncodingSectionHandler,
              Mono.Http, Version=1.0.5000.0,
              PublicKeyToken=0738eb9f132ed756" />
     </sectionGroup>
  </configSections>
-->
<system.web>
```

```
   <customErrors mode="Off"/>
   <httpRuntime
       executionTimeout="3400"
       maxRequestLength="2097152"
   />
<!-- take this out until we need it
  <webServices>
    <soapExtensionTypes>
      <add type="DumpExtension, extensions" priority="0" group="0" />
      <add type="EncryptExtension, extensions" priority="1"
           group="0" />
    </soapExtensionTypes>
  </webServices>
-->
  <authentication mode="None">
  </authentication>
  <httpModules>
    <add name="AuthenticationModule"
       type="Simias.Security.Web.AuthenticationModule, SimiasLib"/>
  </httpModules>
  <httpHandlers>
     <add verb="*" path="admindata/*.log"
        type="Simias.Server.ReportLogHandler,Simias.Server"/>
     <add verb="*" path="admindata/*.csv"
        type="Simias.Server.ReportLogHandler,Simias.Server"/>
  </httpHandlers>
</system.web>
<system.net>
  <connectionManagement>
    <add address="*" maxconnection="10" />
  </connectionManagement>
</system.net>
<!--
<mono.aspnet>
   <acceptEncoding>
   <add encoding="gzip"
        type="Mono.Http.GZipWriteFilter, Mono.Http, Version=1.0.5000.0,
            PublicKeyToken=0738eb9f132ed756" disabled="no" />
```

```
   </acceptEncoding>
</mono.aspnet>
-->
<appSettings>
    <add key="MonoServerDefaultIndexFiles" value="index.aspx,
              Default.aspx,default.aspx, index.html, index.htm" />
    <add key="SimiasCert" value="" />
</appSettings>
</configuration>
```

C.3 Web.config File for the Web Admin Server

By default, the Web.config file for Web Admin server is in the `/usr/lib/simias/admin`. The following is an example of a configured file.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <system.web>
    <httpRuntime executionTimeout="180" maxRequestLength="10240" />
<!--  DYNAMIC DEBUG COMPILATION
      Set compilation debug="true" to enable ASPX debugging.
      Otherwise, setting this value to false will improve runtime
         performance of this application.Set compilation debug="true"
         to insert debugging symbols (.pdb information)into the
          compiled page. Because this creates a larger file that
         executes more slowly,you should set this value to true
         only when debugging and to false at all other times.
         For more information, refer to the documentation about
         debugging SP.NET files.
    -->
    <compilation defaultLanguage="C#" debug="true" />
    <!--  CUSTOM ERROR MESSAGES
          Set customErrors mode="On" or "RemoteOnly" to enable custom
          error messages, "Off" to disable.
          Add <error> tags for each of the errors you want to handle.
          "On" Always display custom (friendly) messages.
          "Off" Always display detailed ASP.NET error information.
          "RemoteOnly" Display custom (friendly) messages only to users
          not running on the local Web server. This setting is
          recommended for security purposes, so that you do not display
```

```
     application detail information to remote clients.
 -->
 <customErrors defaultRedirect="Error.aspx" mode="On" />
 <!--  AUTHENTICATION
       This section sets the authentication policies of the
       application. Possible modes are
       "Windows", "Forms", "Passport" and "None".
       "None" No authentication is performed.
       "Windows" IIS performs authentication (Basic, Digest, or
       Integrated Windows) according to its settings for the
       application. Anonymous access must be disabled in IIS.
       "Forms" You provide a custom form (Web page) for users to
       enter their credentials, and then you authenticate them in
       your application. A user credential token is stored
       in a cookie.
       "Passport" Authentication is performed via a centralized
       authentication service provided by Microsoft that offers a
       single logon and core profile services for member sites.
 -->
 <authentication mode="Forms">
   <forms name="iFolderWebAuth" loginUrl="Login.aspx" timeout="20"
          slidingExpiration="true"  />
 </authentication>
<!--  AUTHORIZATION
       This section sets the authorization policies of the
       application. You can allow or deny access to application
       resources by user or role.
       Wildcards:
         "*" mean everyone,
         "?" means anonymous (unauthenticated) users.
 -->
 <authorization>
   <deny users="?" />
 </authorization>
 <!--  APPLICATION-LEVEL TRACE LOGGING
       Application-level tracing enables trace log output for every
       page within an application.
```

```
        Set trace enabled="true" to enable application trace logging.
        If pageOutput="true", the trace information will be displayed
        at the bottom of each page.  Otherwise, you can view the
        application trace log by browsing the "trace.axd" page from
        your web application root.
  -->
  <trace enabled="false" requestLimit="10" pageOutput="false"
         traceMode="SortByTime" localOnly="true" />
  <!--  SESSION STATE SETTINGS
        By default ASP.NET uses cookies to identify which requests
        belong to a particular session. If cookies are not available,
        a session can be tracked by adding a session
        identifier to the URL. To disable cookies, set
        sessionState cookieless="true".
  -->
  <sessionState mode="InProc" cookieless="false" timeout="20" />
  <httpHandlers>
    <add verb="*" path="tail/*.log"
         type="Novell.iFolderWeb.Admin.LogTailHandler,Novell.iFolderAdmin" />
    <add verb="*" path="*.log"
         type="Novell.iFolderWeb.Admin.ReportLogHandler,Novell.iFolderAdmin" />
    <add verb="*" path="*.csv"
         type="Novell.iFolderWeb.Admin.ReportLogHandler,Novell.iFolderAdmin" />
  </httpHandlers>
  <!--  GLOBALIZATION
        This section sets the globalization settings of the
        application.
  -->
  <globalization requestEncoding="utf-8" responseEncoding="utf-8" />
</system.web>
<appSettings>
  <add key="SimiasUrl" value="https://localhost" />
  <add key="SimiasCert" value="a_certification_key_goes_here" />
</appSettings>
<location path="Default.aspx">
  <system.web>
    <authorization>
      <allow users="*" />
    </authorization>
```

```
    </system.web>
  </location>
  <location path="Error.aspx">
    <system.web>
      <authorization>
        <allow users="*" />
      </authorization>
    </system.web>
  </location>
</configuration>
```

C.4 Web.config File for the Web Access Server

By default, the `Web.config` file for the Web Access server is in the `/opt/novell/ifolder3/lib/simias/webaccess/` directory. The following is an example of a configured file.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <system.web>
    <httpRuntime executionTimeout="3400" maxRequestLength="2097152" />
    <!--  DYNAMIC DEBUG COMPILATION
          Set compilation debug="true" to enable ASPX debugging.
          Otherwise, setting this value to false will improve runtime
          performance of this application. Set compilation
          debug="true" to insert debugging symbols (.pdb information)
          into the compiled page. Because this creates a larger file
          that executes more slowly, you should set this value to true
           only when debugging and to false at all other times. For more
          information, refer to the documentation about debugging
          ASP.NET files.
    -->
    <compilation defaultLanguage="C#" debug="true" />
    <!--  CUSTOM ERROR MESSAGES
          Set customErrors mode="On" or "RemoteOnly" to enable custom
          error messages, "Off" to disable.
          Add <error> tags for each of the errors you want to handle.
          "On" Always display custom (friendly) messages.
          "Off" Always display detailed ASP.NET error information.
          "RemoteOnly" Display custom (friendly) messages only to users
```

```
      not running on the local Web server. This setting is
      recommended for security purposes, so that you do not display
     application detail information to remote clients.
 -->
 <customErrors defaultRedirect="Error.aspx" mode="RemoteOnly" />
 <!--  AUTHENTICATION
      This section sets the authentication policies of the
      application. Possible modes are
      "Windows", "Forms", "Passport" and "None".
      "None" No authentication is performed.
      "Windows" IIS performs authentication (Basic, Digest, or
      Integrated Windows) according to its settings for the
      application. Anonymous access must be disabled in IIS.
      "Forms" You provide a custom form (Web page) for users to
      enter their credentials, and then you authenticate them in
      your application. A user credential token is stored
      in a cookie.
      "Passport" Authentication is performed via a centralized
      authentication service provided by Microsoft that offers a
      single logon and core profile services for member sites.
 -->
 <authentication mode="Forms">
   <forms name="iFolderWeb" loginUrl="Login.aspx" timeout="20"
          slidingExpiration="true"  />
 </authentication>
<!--  AUTHORIZATION
      This section sets the authorization policies of the
      application. You can allow or deny access to application
      resources by user or role.
      Wildcards:
        "*" mean everyone,
        "?" means anonymous (unauthenticated) users.
 -->
 <authorization>
   <deny users="?" />
 </authorization>
 <!--  APPLICATION-LEVEL TRACE LOGGING
```

```
        Application-level tracing enables trace log output for every
        page within an application.
        Set trace enabled="true" to enable application trace logging.
        If pageOutput="true", the trace information will be displayed
        at the bottom of each page.  Otherwise, you can view the
        application trace log by browsing the "trace.axd" page from
        your web application root.
  -->
  <trace enabled="false" requestLimit="10" pageOutput="false"
         traceMode="SortByTime" localOnly="true" />
  <!--  SESSION STATE SETTINGS
        By default ASP.NET uses cookies to identify which requests
        belong to a particular session. If cookies are not available,
        a session can be tracked by adding a session
        identifier to the URL. To disable cookies, set
        sessionState cookieless="true".
  -->
  <sessionState mode="InProc" cookieless="false" timeout="30" />
  <!--  GLOBALIZATION
        This section sets the globalization settings of the
        application.
  -->
  <globalization requestEncoding="utf-8" responseEncoding="utf-8" />
  <httpModules>
    <add name="UploadModule" type="Novell.iFolderApp.Web.UploadModule,
         Novell.iFolderWeb" />
  </httpModules>
</system.web>
<appSettings>
  <add key="SimiasUrl" value="https://localhost" />
  <add key="SimiasCert" value="a_certification_key_goes_here" />
</appSettings>
<location path="Default.aspx">
  <system.web>
    <authorization>
      <allow users="*" />
    </authorization>
  </system.web>
```

```
  </location>
  <location path="ICLogout.aspx">
    <system.web>
      <authorization>
        <allow users="*" />
      </authorization>
    </system.web>
  </location>
</configuration>
```

D Managing SSL Certificates for Apache

This section discusses how to acquire and manage SSL certificates for Novell iFolder servers.

- Section D.1, “Generating an SSL Certificate for the Server,” on page 221
- Section D.2, “Generating a Self-Signed SSL Certificate for Testing Purposes,” on page 222
- Section D.3, “Configuring Apache to Point to an SSL Certificate on an iFolder Server,” on page 222
- Section D.4, “Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster,” on page 223
- Section D.5, “Replacing the SSL Certificate for an iFolder Enterprise Server,” on page 224

D.1 Generating an SSL Certificate for the Server

Using SSL requires that you install an SSL certificate form on each iFolder enterprise server, Web Admin server and Web Access server in your domain. Users accept the certificates to enable communications with the servers.

The certificate can be a self-signed certificate or a certificate from a trusted certificate authority. A self-signed certificate is usually used only for internal iFolder services, where the server’s identity is not likely to be spoofed. The trusted CA signature on the certificate attests that the public key contained in the certificate belongs to the person, organization, server, or other entity noted in the certificate. It assures users that they are accessing a valid, non-spoofed resource. If the information does not match or the certificate has expired, an error message warns the user.

Browsers are typically preconfigured to trust well-known certificate authorities. If you use a Certificate Authority that is not configured into browsers by default, it is necessary to load the Certificate Authority certificate into the browser, enabling the browser to validate server certificates signed by that Certificate Authority.

To acquire SSL certificates for use in an operational public-key infrastructure (PKI), use one of the following methods, depending on your network needs:

- Use the self-signed certificate that is created and enabled for the server by default during the server install.
- Use the services of a third-party certificate authority to get trusted certificate, then use it instead of accepting the default certificate during the sever install.

Whichever method you use, the certificate is automatically used for the Apache Web Server configuration. If it does not automatically configure the certificate for the Apache Web Server, see the following:

- Section D.3, “Configuring Apache to Point to an SSL Certificate on an iFolder Server,” on page 222
- Section D.4, “Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster,” on page 223

D.2 Generating a Self-Signed SSL Certificate for Testing Purposes

You can use the YaST CA Management plug-in or OpenSSL tools to create a self-signed certificate. If iFolder is deployed in a trusted environment, use YaST. The YaST CA Management interface contains modules for the basic management of X.509 certificates. This mainly involves the creation of CAs, sub-CAs, and their certificates. For more information, see the following:

- Section 6.7.2, “Creating a YaST-based CA,” on page 88
- Section 6.7.3, “Creating Self-Signed Certificates Using YaST,” on page 90
- Section 6.7.4, “Exporting Self-Signed Certificates,” on page 92

For detailed information about how to generate a certificates, see Creating a Self-Signed Certificate (http://www.suse.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/sec_apache2_ssl.html) in the *SUSE Linux Enterprise Server 11 Administration Guide* (http://www.suse.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html).

For information about configuring Apache to point to the self-signed certificate, see the following:

- Section D.3, “Configuring Apache to Point to an SSL Certificate on an iFolder Server,” on page 222
- Section D.4, “Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster,” on page 223

D.3 Configuring Apache to Point to an SSL Certificate on an iFolder Server

1. Get an SSL certificate from a trusted certificate authority.
2. Create a shared key directory. At a terminal console, enter

   ```
   mkdir /etc/sharedkey/
   ```

   Replace `sharedkey` with the actual name of your key directory.
3. Do either of the following:
   - Copy the private key (`.key` file) and the certificate (`.cert` file) to the shared key directory location. At a terminal console, enter

     ```
     cp ./filename.key /etc/sharedkey/
     cp ./filename.cert /etc/sharedkey/
     ```

     Replace *`filename`* with the actual file name of your `.key` and `.cert` files. Replace the destination path with the shared key directory location where you want to store the `.key` and `.cert` files.
   - If you have received a single `.pem` file from the trusted authority, copy that to the shared key directory location. At a terminal console, enter

     ```
     cp ./filename.pem /etc/sharedkey/
     ```
4. Perform either of the following:

   4a Edit the Apache SSL configuration file (`/etc/apache2/vhosts.d/vhost-ssl.conf`) to point to the `.key` file and `.cert` file by modifying the values for the following parameters:

```
SSLCertificateKeyFile=/etc/sharedkey/filename.key
```

```
SSLCertificateFile=/etc/sharedkey/filename.cert
```

Replace the path to the files with the actual location and filenames.

4b Edit the Apache SSL configuration file (`/etc/apache2/vhosts.d/vhost-ssl.conf`) to point to the `.pem` file by modifying the values for the following parameters:

```
SSLCertificateKeyFile=/etc/sharedkey/filename.pem
```

```
SSLCertificateFile=/etc/sharedkey/filename.pem
```

WARNING: Ensure that there are no duplicate entries for `SSLCertificateKeyFile` and `SSLCertificateFile` in the Apache SSL configuration file.

---

5 Restart the Apache server.

D.4 Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster

Use this configuration when one pool is serving all services. This configuration is not useful when each service uses separate pools.

1 Mount the shared volume. At a terminal console, enter

```
mnt /dev/sda1 /mnt/ifolder3
```

Replace `/dev/sda1` with the actual disk or partition containing the file system. Replace `/mnt/ifolder3` with the mount point (directory path) of the shared volume.

2 Do either of the following:

- Copy the private key (`.key` file) and the certificate (`.cert` file) to a location on the mounted shared volume. At a terminal console, enter

```
cp ./filename.key /mnt/ifolder3/sharedkey/
```

```
cp ./filename.cert /mnt/ifolder3/sharedkey/
```

Replace `filename` with the actual file name of your `.key` and `.cert` files. Replace the destination path with the location where you want to store the shared key and certificate files.

- If you have received a single `.pem` file from the trusted authority, copy that to the shared keydirectory location. At a terminal console, enter

```
cp ./filename.pem /mnt/ifolder3/sharedkey/
```

3 Do either of the following:

- Edit the Apache SSL configuration file (`/etc/apache2/vhosts.d/vhost-ssl.conf`) to point to the `.key` file and `.cert` file by modifying the values for the following parameters:

```
SSLCertificateKeyFile=/mnt/ifolder3/sharedkey/filename.key
```

```
SSLCertificateFile=/mnt/ifolder3/sharedkey/filename.cert
```

Replace the path to the files with the actual location and filename on the shared volume.

- Edit the Apache SSL configuration file (`/etc/apache2/vhosts.d/vhost-ssl.conf`) to point to the `.pem` file by modifying the values for the following parameters:

```
SSLCertificateKeyFile=/mnt/ifolder3/sharedkey/filename.pem
```

`SSLCertificateFile=/mnt/ifolder3/sharedkey/filename.pem`

WARNING: Ensure that there are no duplicate entries for `SSLCertificateKeyFile` and `SSLCertificateFile` in the Apache SSL configuration file.

4 Restart the Apache server.

NOTE: Ensure that the shared volume is mounted before you start the Apache server.

D.5 Replacing the SSL Certificate for an iFolder Enterprise Server

This section discusses how to replace the SSL certificate for a single iFolder server, iFolder master server, and iFolder slave server.

- Section D.5.1, "Replacing the SSL Certificate for a Single iFolder Server," on page 224
- Section D.5.2, "Replacing the SSL Certificate for an iFolder Master Server," on page 225
- Section D.5.3, "Replacing the SSL Certificate for an iFolder Slave Server," on page 225

D.5.1 Replacing the SSL Certificate for a Single iFolder Server

1. Create a backup of the original certificate from the Apache certificate store.
2. Ensure you have the valid new certificate to replace the original certificate.
3. If the names of the original and new certificates differ, edit the `/etc/apache2/vhosts.d/vhost-ssl.conf` file and replace the filename of the original certificate with that of the new certificate.
4. Create a backup of the `/opt/novell/ifolder3/%lib/simias/admin/Web.config` and `/opt/novell/ifolder3/%lib/simias/webaccess/Web.config` files. Here, `%lib` must be replaced by lib for the 32-bit server and lib64 for the 64-bit servers.
5. Copy the new certificate to the Apache certificate store. The permission assigned on the new certificate must be same as the permission for the original certificate.
6. Restart Apache.
7. Configure the iFolder Web Admin sever and the Web Access server to import the new certificate keys in the admin `Web.config` file.
8. Restart Apache.
9. Log in to the Web Admin console and Web Access console to verify if you are able to successfully view all the pages in the Web Admin and Web Access console.

D.5.2 Replacing the SSL Certificate for an iFolder Master Server

To replace the certificate of an iFolder master server in a multi-server deployment, you must first replace the certificate on the master server by using the procedure in Section D.5.1, “Replacing the SSL Certificate for a Single iFolder Server,” on page 224, then follow the steps given below to change the slave server configurations. Because of the change in the configuration, the slave servers start using the new certificate from the master server.

1. Navigate to the iFolder slave server directory `/opt/novell/ifolder3/%lib/simias/web` and create a backup of the `web.config` file. Here, `%lib` must be replaced by lib for the 32-bit server and lib64 for the 64-bit server.
2. Create a backup of the `web.config` file.
3. On the master server, open the `Web.config` file at the location `/opt/novell/ifolder3/%lib/simias/admin/` and copy the value of the SimiasCert XML attribute. On the slave server, open the `web.config` file at the location `/opt/novell/ifolder3/%lib/simias/web/` and replace the value of the XML attribute SimiasCert with the value copied from the master server.
4. Restart Apache on the slave server.
5. Log in to the slave server Web Admin console to verify if you can successfully view all the pages.

D.5.3 Replacing the SSL Certificate for an iFolder Slave Server

To replace certificate on an iFolder slave server, you can use the procedure outlined in Section D.5.1, “Replacing the SSL Certificate for a Single iFolder Server,” on page 224. There is no need to modify any configuration file on the iFolder master server if only the slave server certificate needs to be replaced.

E Product History of iFolder 3

This section compares the different versions of Novell iFolder 3.*x* to clarify which operating systems, directories, and other components are supported in each.

- Section E.1, “Version History,” on page 227
- Section E.2, “Network Operating Systems Support,” on page 228
- Section E.3, “Workstation Operating Systems Support for the iFolder Client,” on page 228
- Section E.4, “Server Client Support,” on page 229
- Section E.5, “Web Server Support,” on page 229
- Section E.6, “iFolder User Access Support,” on page 230

For a comparison of features in 2.1*x* and 3.*x*, see Chapter 4, “Comparing Novell iFolder 2.x with 3.9,” on page 37.

E.1 Version History

Table E-1 *Version History*

Version	Type	Description
3.6	Bundled	Provides support for OES 2 servers. Provides support to upgrade from previous iFolder 3.x clients to an iFolder 3.6 client and migrate from iFolder 2.*x* clients to an iFolder 3.6 client.
3.7	Bundled	Provides support for Multi-server, UserMove, SSL and client enhancement like Mac and Vista support.
3.8	Bundled	Provides support for Multi-level administration, Active Directory integration for iFolder, Passphrase Recovery Wizard, enhanced user interface.
3.8.4	Bundled	Provides support for OES common proxy and to upgrade a slave server to a master server. The iFolder data recovery tool is also available with this version.
3.9	Bundled	Provides support for OES 11 on SLES 11 SP1 64-bit platform.
3.9.1	Bundled	Provides support for OES 11 SP1 (SLES 11 SP2) and OES 11 SP2 (SLES 11 SP3) 64-bit platform.
3.9.2	Bundled	Provides support for OES 11 SP1 (SLES 11 SP2), OES 11 SP2 (SLES 11 SP3), and OES 2015 (SLES 11 SP3) 64-bit platform.

E.2 Network Operating Systems Support

Table E-2 Network Operating Systems

Network Operating System	3.6	3.7	3.8	3.8.4	3.9	3.9.1	3.9.2
OES 2.0	Yes	No	No	No	No	No	No
OES 2 SP1	No	Yes	No	No	No	No	No
OES 2 SP2	No	No	Yes	No	No	No	No
OES 2 SP3	No	No	No	Yes	No	No	No
OES 11	No	No	No	No	Yes	No	No
OES 11 SP1	No	No	No	No	No	Yes	No
OES 11 SP2	No	No	No	No	No	No	Yes
OES 2015	No	No	No	No	No	No	Yes

E.3 Workstation Operating Systems Support for the iFolder Client

Table E-3 Workstation Operating Systems

Workstation Operating System	3.6	3.7	3.8	3.8.4	3.9	3.9.1	3.9.2
SUSE Linux Enterprise Desktop 10 SP3	No	No	No	Yes	Yes	No	No
SUSE Linux Enterprise Desktop 11	No	No	Yes	No	No	No	No
SUSE Linux Enterprise Desktop 11 SP1	No	No	No	Yes	Yes	No	No
SUSE Linux Enterprise Desktop 11 SP2	No	No	No	Yes	Yes	Yes	Yes

Workstation Operating System	3.6	3.7	3.8	3.8.4	3.9	3.9.1	3.9.2
Windows	Win XP SP2/ 2000	Win XP SP2/ Vista SP1	Win XP SP2/Vista SP1/Win7	Win XP SP3/Vista SP1 /Win 7	Win XP SP3/ Vista SP1/ Win 7	Win XP SP3/ Vista SP1/ Win 7	Win XP SP3/ Win 7/ Win 8
Macintosh OS X v10.3 and later	No	10.4	10.4, 10.5	10.5, 10.6	10.5, 10.6	10.5, 10.6, 10.7	10.6, 10.7, 10.8, 10.9
open SUSE 12.1	No	No	No	No	No	Yes	No

E.4 Server Client Support

Table E-4 *Server Client Support Matrix*

Server Version	Client Version
3.7	3.7.*x*
3.8	3.8.*x*
3.9	3.9.*x*

E.5 Web Server Support

Table E-5 *Web Server Support*

Web Server	3.6	3.7	3.8	3.8.4	3.9	3.9.1	3.9.2
Apache	2 (worker mode)	2 (worker mode)	2 (worker mode)	2 (worker mode)	2 (worker mode)	2 (worker mode)	2 (worker mode)

E.6 iFolder User Access Support

Table E-6 *iFolder User Access Support*

iFolder User Access Method	3.6	3.7	3.8	3.8.4	3.9	3.9.1	3.9.2
Novell iFolder 3.x Web Access	IE 6.0/7.0 Firefox Safari	IE 6.0/7.0 Firefox Safari	IE 6.0/7.0 Firefox Safari	IE 8.0 Firefox 3.6 Safari 4.x/5.x	IE 8.0 Firefox 3.6.x Safari 4.x/5.x	IE 8.0 Firefox 3.6.x Safari 4.x/5.x	IE Firefox Safari
Novell iFolder Web Admin	IE 6.0/7.0 Firefox Safari	IE 6.0/7.0 Firefox Safari	IE 6.0/7.0 Firefox Safari	IE 8.0 Firefox 3.6 Safari 4.x/5.x	IE 8.0 Firefox 3.6 Safari 4.x/5.x	IE 8.0 Firefox 3.6.x Safari 4.x/5.x	IE Firefox Safari

F Documentation Updates

This section contains information about documentation content changes made to the *Novell iFolder 3.x Administration Guide*. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date, which appears on the front cover and the Legal Notices page, to determine the release date of this guide. For the most recent version of the *Novell iFolder 3.9.x Administration Guide*, see the Novell iFolder 3.*x* documentation Web site (http://www.novell.com/documentation/ifolder3/index.html).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped and sequenced, according to where they appear in the document itself. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:

- Section F.1, “August 2015,” on page 231
- Section F.2, “January 2014,” on page 231
- Section F.3, “August 2012,” on page 232
- Section F.4, “July 2011,” on page 232
- Section F.5, “December 2010,” on page 233
- Section F.6, “June 2010,” on page 233
- Section F.7, “August 2009,” on page 234
- Section F.8, “October 2008,” on page 235

F.1 August 2015

This guide is modified with OES 2015 changes.

F.2 January 2014

From OES 11 SP2 onwards, OpenSUSE is not supported as iFolder client. Hence, all the references of OpenSUSE for this release are removed.

Updates were made to the following section.

F.2.1 Installing and Configuring iFolder Services

Location	Change
Section 6.2.1, “Configuring the iFolder Enterprise Server,” on page 52	Moved Step 8 - NSS file system trustee rights and made it Step 2.

Location	Change
Section 6.12, “Updating Novell iFolder 3.9.x,” on page 106	This section is modified to delete the version configuration file details.

F.2.2 Troubleshooting Tips For Novell iFolder

Location	Change
Section 15.1, “On Upgrading the Server from OES 2 SP3 to OES 11, iFolder Fails to Function,” on page 192	New issue

F.2.3 Product History of iFolder 3

Location	Change
Appendix E, “Product History of iFolder 3,” on page 227	◆ Updated this section to reflect version 3.9.2 ◆ Removed the versions earlier than 3.6

F.3 August 2012

Updates were made to the following section. The changes are explained below.

F.3.1 What’s New in iFolder

Location	Change
Section 2.2, “What’s New in Novell iFolder 3.9.1,” on page 23	This section is new.

F.3.2 Product History of iFolder 3

Location	Change
Appendix E, “Product History of iFolder 3,” on page 227	Updated this section to reflect version 3.9.1

F.4 July 2011

Updates were made to the following section. The changes are explained below.

F.4.1 Managing an iFolder Enterprise Server

Location	Change
Section 10.10.2, “Prerequisites and Guidelines,” on page 136	Updated this section with new guideline, “Files are restored from iFolder and its immediate subfolder. The subsequent subfolders cannot be restored.”
Section 10.10.3, “Using the Data Recovery Tool,” on page 136	Deleted the short options for the Data Recovery Tool.
“Restoring a Subfolder” on page 138	Added new paragraph that subsequent subfolders cannot be restored.

F.5 December 2010

Updates were made to the following section. The changes are explained below.

F.5.1 Replacing the SSL Certificates

The following changes was made to this section:

Location	Change
Section D.5, “Replacing the SSL Certificate for an iFolder Enterprise Server,” on page 224	Added a new section that outlines the procedure to replace the SSL certificates for single iFolder server and multi-iFolder server setup.

F.6 June 2010

Updates were made to the following section. The changes are explained below.

F.6.1 iFolder Data Recovery Tool

The following change was made to this section:

Table F-1 *iFolder Data Recovery Tool*

Location	Change
Section 10.10, “iFolder Data Recovery Tool,” on page 135	Added a new section on iFolder Data Recovery tool. This section describes the features of this tool and use case scenarios that explain the usage of this tool in detail.

F.6.2 Upgrade Slave to Master

The following change was made to this section:

Table F-2 Active Directory Integration for iFolder

Location	Change
Section 11.5.2, "Upgrading a Slave Server to a Master Server," on page 165	Added a new section that outlines the procedure to upgrade a slave server to a master server.

F.7 August 2009

Updates were made to the following section. The changes are explained below.

F.7.1 Multi-Level Administration

The following change was made to this section:

Table F-3 Multi-Level Administration

Location	Change
"Multi-level administration" on page 152	Added a new section on Multi-Level Administration. This section describes the concept of primary and secondary administrators.

F.7.2 Active Directory Integration for iFolder

The following change was made to this section:

Table F-4 Active Directory Integration for iFolder

Location	Change
Section 5.4, "Active Directory," on page 46	Modified the existing content to delete existing workarounds for Active Directory integration with iFolder.

F.7.3 Installation of iFolder on SLED and Windows Using ZENworks

The following change was made to this section:

Table F-5 Installation of iFolder on SLED and Windows Using ZENworks

Location	Change
"Installation of iFolder on SLED using ZENworks Linux Management" on page 103	Added a new section on installation of iFolder on SLED using ZENworks.
"Installation of iFolder on Windows using ZENworks Configuration Management" on page 104	Added a new section on installation of iFolder on Windows using ZENworks.

F.8 October 2008

Updates were made to the following section. The changes are explained below.

- Section F.8.1, “LDAP Group Support,” on page 235
- Section F.8.2, “Recovery Agent Certificates,” on page 235
- Section F.8.3, “Recovering iFolder Data from File System Backup,” on page 235
- Section F.8.4, “Viewing Reprovisioning Status,” on page 236
- Section F.8.5, “SSL Communications,” on page 236
- Section F.8.6, “Simias.config File,” on page 236
- Section F.8.7, “Web.config File for the Web Admin Server,” on page 237

F.8.1 LDAP Group Support

The following change was made to this section:

Table F-6 *LDAP Group Support*

Location	Change
Section 3.5.3, “Synchronizing LDAP Group Accounts with LDAP,” on page 31	Added a new section on synchronizing LDAP Groups with the LDAP server.
Section 1.1.12, “LDAP Group Support,” on page 16	Added support for LDAP Groups.
Section 12.1, “Provisioning / Reprovisioning Users and LDAP Groups for iFolder,” on page 169	Provisioning users and LDAP Groups.
Table 12-1 on page 171	Update the table with information on user groups and group members.

F.8.2 Recovery Agent Certificates

The following change was made to this section:

Table F-7 *Recovery Agent Certificates*

Location	Change
Section 6.7, “Recovery Agent Certificates,” on page 87	Added a new section on Recovery Agent Certificates. This section describes how to create a recovery agent certificate and the process for recovering the key.

F.8.3 Recovering iFolder Data from File System Backup

The following change was made to this section:

Table F-8 Recovering iFolder Data

Location	Change
Section 10.8.1, “Recovering a Regular iFolder,” on page 133	Added a new section.

F.8.4 Viewing Reprovisioning Status

The following change was made to this section:

Table F-9 Reprovisioning Status

Location	Change
Section 11.4.2, “Viewing Reprovisioning Status,” on page 151	Added a new section on viewing the reprovisioning status of the users by using the Web Admin console.

F.8.5 SSL Communications

The following change was made to this section:

Table F-10 SSL Communications

Location	Change
Section 10.12.5, “Configuring the Enterprise Server for SSL Communications with the Web Access Server and Web Admin Server,” on page 145	Added a new section on configuring iFolder server for SSL communications with the Web consoles.
Section 11.6.3, “Configuring the Web Admin Server for SSL Communications with the Enterprise Server,” on page 167	Added new section on configuring Web Admin server for SSL communication with iFolder server.
Section 11.6.4, “Configuring the Web Admin Server for SSL Communications with Web Browsers,” on page 167	Added new section on configuring Web Admin server for SSL communication with Web Browsers.
Section 11.6.5, “Configuring an SSL Certificate for the Web Admin Server,” on page 168	Added new section on configuring SSL certificate for Web Admin server.

F.8.6 Simias.config File

The following change was made to this section:

Table F-11 simias.config files

Location	Change
Section C.1, “Simias.config File,” on page 211	Updated the simias.config file.

F.8.7 Web.config File for the Web Admin Server

The following change was made to this section:

Table F-12 *Web Config Files*

Location	Change
Section C.3, “Web.config File for the Web Admin Server,” on page 214	Added a new section for Web.config files for the Web Admin server.